

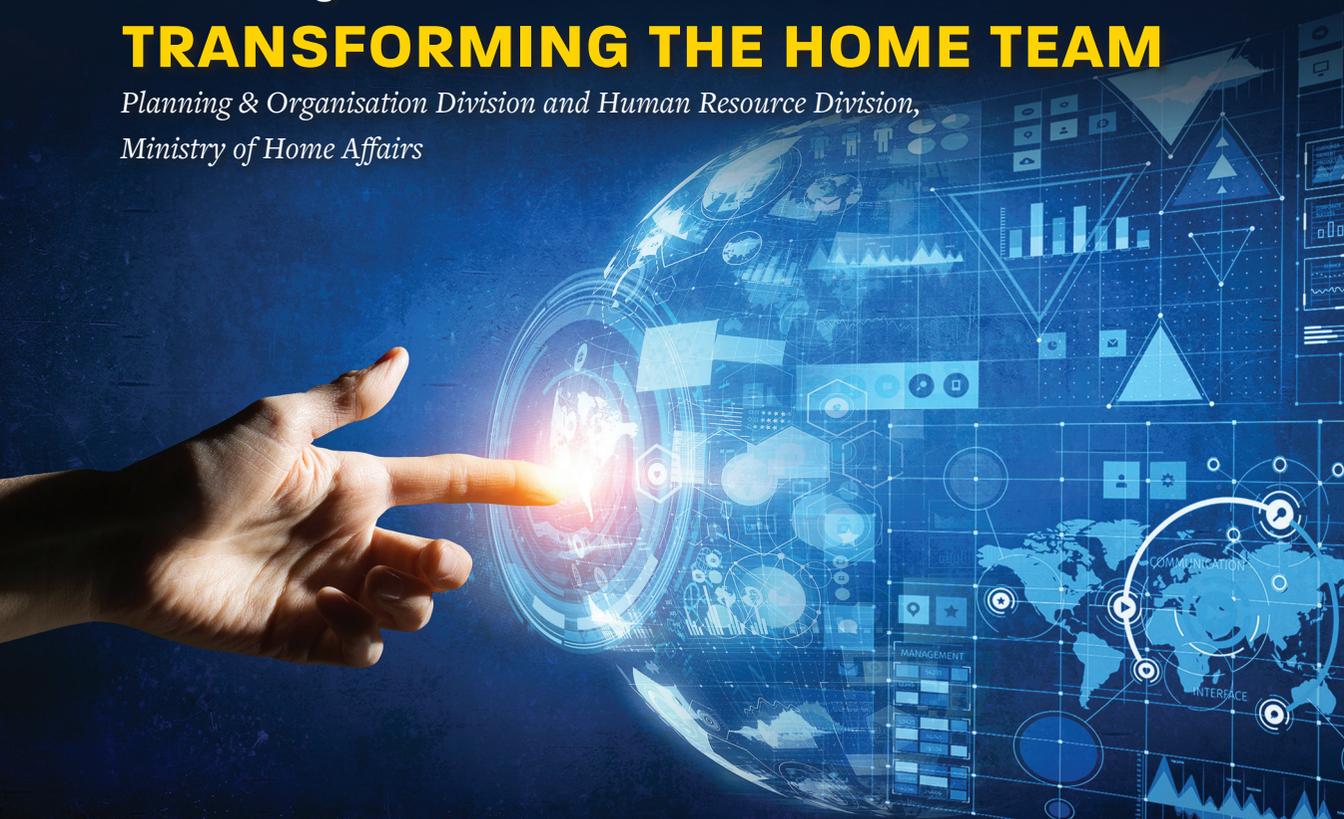
HOME TEAM JOURNAL

BY PRACTITIONERS,
FOR PRACTITIONERS

Cover Story

TRANSFORMING THE HOME TEAM

*Planning & Organisation Division and Human Resource Division,
Ministry of Home Affairs*



THE GROWING NEED FOR ADVOCACY AGAINST ILLICIT DRUGS

Dr. Rozlan Giri, Sivaraman Letchumanan and Nur Asyikin Hamzah

Special Feature on Counter-Terrorism

THE PSYCHOLOGY BEHIND SINGAPORE'S TERRORIST REHABILITATION STRATEGY AND BEST PRACTICES IN COUNTERING VIOLENT EXTREMISM

Counter-Terrorism Division, Internal Security Department

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. The journal publishes articles and reviews on issues relating to the Home Team and its core competencies.

It aims to be a platform to share knowledge and new insights, stimulate critical thinking and discussion among the Home Team community, and reach out to our stakeholders and the global community of practitioners in national safety and security.



EDITORIAL BOARD

CHAIRPERSON

T. Raja Kumar

DEPUTY CHAIRPERSON

Teo Tze Fang

CHIEF EDITOR

Winston Wong Sung-En

DEPUTY CHIEF EDITOR

Lim Jing Jing

EDITORIAL CONSULTANT

Susan Sim

DEPARTMENTAL EDITORS

Elton Yeo

Gobiselven Govindasamy

Jane Quek

Jasmin Kaur

Jaswant Singh

Raymond Lim

Suhara

Tan Teck Tien

Winsome Chow

Please address all contributions and correspondence to:

Home Team Journal Editorial Board

Planning and Organisation Development Centre

Home Team Academy

501 Old Choa Chu Kang Road, Singapore 698928

For comments and feedback, please mail to

MHA_HT_Journal@mha.gov.sg

CONTENTS

HOME TEAM ACADEMY • 2018 ISSUE NO 7

FOREWORD	04	by Loh Ngai Seng
INTRODUCTION BY CHAIRPERSON	05	by T. Raja Kumar
COVER STORY	07	Transforming the Home Team Planning & Organisation Division and Human Resource Division, Ministry of Home Affairs
TECHNOLOGY	18	Harnessing the Power of Technology Dr. Jonathan Pan and Grace Koh
	25	Use of Analytics in Operations Dr. Melvinder Singh and Mark Toh
	31	Use of Virtual Reality Technology in Training: Shazwani Babjee
THOUGHT LEADERSHIP	38	Growing Thought Leadership and Capacity in Safety and Security Jason Jevanathan
	40	Building a Vibrant Eco-system for the Home Team to Deal with Cybersecurity & Cybercrime Threats Michael Ong
	46	The Growing Need for Advocacy against Illicit Drugs
	57	AODC in Action Dr. Rozlan Giri, Sivaraman Letchumanan and Nur Asyikin Hamzah
TERRORISM	70	Evolution of Terrorism Threat to Singapore Counter-Terrorism Division, Internal Security Department
	75	Building the SGSecure Movement Tan Jin Rui Jerald
	81	The Psychology Behind Singapore's Terrorist Rehabilitation Strategy & Best Practices In Countering Violent Extremism Counter-Terrorism Division, Internal Security Department
	87	Comparing ISIS Foreign Fighters versus Sympathisers: Insights from their Twitter Postings Neo Loo Seng, Dr. Majeed Khader, Dr. Joyce S Pang
	107	The Seven Things You Need To Know About Lone-Actor Terrorism Dr. Paul Gill



Copyright ©2018. All rights reserved.

No part of this publication (i.e. 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' own and do not necessarily reflect the opinion of the Home Team Academy.

Foreword



I am delighted to contribute the foreword to this 7th edition of the Home Team Journal. This is a special edition, and a particularly relevant one for all Home Team officers, as it paints a clear and exciting picture of the ongoing Home Team Transformation 2025.

Having served with the Home Team for 15 years, I can say with quiet optimism that the changes are significant. Working together, the Home Team is evolving rapidly to prepare itself for the future.

The Home Team is facing challenges that make transformation not only necessary, but also critical. Traditional crimes now have a new online dimension in the form of transnational cyber-crime. The short time it now takes for an individual to become self-radicalised and the use of readily available tools to cause harm to others combine to make it much harder to prevent a terrorist attack. Drug cartels have moved into new substances and modes of delivery, and we are also grappling with the risks of malicious disinformation posed by fake news.

The Home Team has leveraged technology extensively to equip us with capabilities to deal with these new threats. This starts with a re-think of our concept of operations by each Home Team Department and how the right technology (not necessarily cutting edge) can enable a new way of working. One example is our ability to collect and analyse data effectively to deploy limited resources in a much more targeted and efficient manner.

Our Home Team officers are therefore at the heart of Home Team Transformation 2025. They are the agents of change. Training is the only way to prepare officers to perform their jobs well. My Home Team colleagues know that I like to use the analogy of a professional football team – if football teams only played matches, and did not invest time to train as a team as well as to hone their individual skills, team performance will soon plateau. Thus, making time for training, building a culture where individual officers are motivated and empowered to constantly upgrade their skills, are key to keeping our officers ready and confident to deal with a rapidly-changing operating environment.

Having worked closely with many Home Team officers in driving various pieces of the Home Team Transformation, I have deep respect for their professionalism, sense of mission, and willingness to take risks and drive change. I am confident that under its new leadership, the Home Team will continue to grow from strength to strength, and keep Singapore and Singaporeans safe and secure.

A handwritten signature in black ink, appearing to read 'Loh Ngai Seng'.

Loh Ngai Seng

Permanent Secretary (Transport)

[2nd Permanent Secretary (Home Affairs) from January 2016 to August 2017]

The Journal takes this opportunity to thank Mr Loh Ngai Seng for his service to the Home Team. Mr Loh served in various capacities in the Ministries of Defence, Education and Home Affairs before his appointment as Director of the Internal Security Department in September 2010 and Second Permanent Secretary in the Ministry of Home Affairs in January 2016. As 2PS (Home Affairs), Mr Loh constantly pushed us to reach for new frontiers without losing sight of the mission or the officer. We wish him the best in his new appointment as PS (Transport).

Introduction by Chairman

Since the 1990s, disruptive innovation has impacted lifestyles and up-ended businesses in sectors such as retail, communications, transport and accommodation. The safety and security landscape is also being buffeted by the winds of dramatic change. In an environment rife with volatility, uncertainty, complexity and ambiguity, the Home Team has been thinking and working hard to ensure our continued effectiveness into the next 10 years through the Home Team Transformation 2025 initiative. This 7th issue of the Journal offers a peek into the future of the Home Team, showing how the Home Team and its officers are rising to the challenges that lie ahead.



The first article, co-written by officers from the Planning & Organisation and Human Resource Divisions of the Ministry of Home Affairs, explains the transformation impetus and how the Home Team is managing the changes through strategic workforce planning.

Among the most visible changes arising from the Home Team Transformation 2025 are new technologies that improve our effectiveness. The Home Team has implemented and is trying out a range of technologies. The Singapore Prison Service, for example, has had successes with analytics, Dr. Melvinder Singh and Mark Toh report as they share the lessons they learnt from the development and implementation of two analytics models. The Home Team is also experimenting with virtual reality technology to bring realistic training scenarios to the frontline through MobiC, a mobile classroom using a vehicular platform. In an interview, Dr. Naresh Kumar discusses the genesis of the MobiC project, its design principles and the challenges that the project team had to overcome. As Dr. Jonathan Pan and Grace Koh share in another article, the Home Team is exploring the use of artificial intelligence to analyse data captured by nationwide sensors to support officers in decision-making.

Technology brings with it risks, vulnerabilities and threats. Michael Ong, Executive Director of the Centre for Cyber Security Studies, writes about the importance of engaging collaborators from beyond the Home Team, such as industrial, academic and regional partners, to build a vibrant ecosystem to counter cyber threats. The establishment of the Institute of Safety and Security Studies, which the Centre for Cyber Security Studies is part of, reflects our recognition that operational excellence is no longer sufficient in the current security landscape. The Home Team needs to win hearts and minds, build capabilities and capacity, and strive for thought leadership in the local community, among foreign counterparts, and in the international arena.

For example, we have been effective in containing the local drug problem by adopting a tough and stringent approach against drugs and crime. However, many are unaware that Singapore has adopted a comprehensive approach to tackling drugs and crime – covering prevention, detection, and rehabilitation. Recognising that there is a need to share our story on how we have kept our drug and crime situation under control, an Advocacy Office against Drugs and Crime has been set up under the Institute of Safety and Security Studies to advocate for Singapore's evidence-based approach towards the control of illicit drugs and crime. Dr. Rozlan Giri, Executive Director of the Advocacy Office, explains the urgency of rebuilding the global consensus on drug control in his exposition on the harm reduction movement.

Counter-terrorism is another area where security and enforcement methods alone are insufficient to address the problem holistically. Hence, rehabilitating individual terrorists and carrying out community-wide counter-ideology efforts are two key weapons in our arsenal against terrorism, as explained in an article by psychologists from the Internal Security Department.

Sharing recent research, Dr. Paul Gill explains that lone actor terrorists are generally not true loners. In most cases, other individuals such as family and friends knew about the terrorist's grievances, commitment to an extremist ideology, or intent to carry out acts of terrorism. His findings underline the importance of community engagement. The Home Team has been doing that through SGSecure, a national movement to sensitise, train, and mobilise our community to partner us in the prevention of and response to a terrorist attack.

Much research is also being conducted by our Home Team psychologists on the use of social media by violent extremists, The Journal is thus pleased to publish pioneering research by Neo Loo Seng and Dr. Majeed Khader of the Home Team Behavioural Sciences Centre, and Dr. Joyce Pang of the Nanyang Technological University, to discover tools for identifying readiness to use violence by comparing the Twitter postings of ISIS foreign fighters with sympathisers.

It is my hope that this rich selection of essays, covering the themes of transformation, use of technology, community empowerment, and counter terrorism, show how the Home Team is rapidly evolving and developing its and the community's capabilities to meet the operational and other challenges, and provide readers with much food for thought.



T. Raja Kumar

Chairman

Home Team Journal Editorial Board

TRANSFORMING THE HOME TEAM

By Planning & Organisation Division and Human Resource Division,
Ministry of Home Affairs

This special issue of Home Team Journal looks at how the Home Team has been transforming itself as it gears up to meet emerging challenges and evolving threats. In the first article, the Planning & Organisation and Human Resource Divisions of the Ministry of Home Affairs discuss the driving forces that have made Home Team Transformation 2025 an urgent imperative and explain the processes underway to develop the Next-Gen Home Team Officer.

In March 2015, then Permanent Secretary (Home Affairs) Leo Yip chaired the first Strategic Planning and Resource Management meeting in the Tanglin Conference Room at New Phoenix Park, kick-starting the formal process of planning for the long term across the entire Home Team. The imperatives were clear. The scale and nature of the challenges ahead required transformative change, not just tweaks and refinements, he told his leadership team. But transformative change took time, especially if new capabil-

“ Will the Home Team be as effective in the year 2025? Will we still be on top of our challenges in ten years’ time? Will we cope well with rising workload, or will we be overwhelmed? Can we effectively harness exciting new technologies, or will we be lagging behind? Can we deal effectively with the implications of an ageing population and a very tight manpower situation?

If the answer to all these questions is to be “Yes”, we need to work hard to make it happen. We know for a fact that the environment we operate in, in the year 2025 will be very different from today. It must then follow that for the Home Team to remain effective, we cannot operate in 2025 the way we work today. ”

– Leo Yip, Permanent Secretary
Ministry of Home Affairs (2014-2017)

Home Team Transformation 2025



The Home Team is transforming for a future of higher load and lower manning



Source: HT Transformation 2025, *Home Team News Bytes*, an e-bulletin distributed to Home Team officers

ities were to be planned for and developed, particularly in an operational ministry like the Ministry of Home Affairs. The time to push ahead with new ideas and new technologies was not five years or eight years hence, but immediately. Home Team Transformation 2025 was already happening.

Over successive meetings, Home Team planners repeatedly asked themselves fundamental questions such as: What will policing, emergency response, drug control, corrections, border security and other Home Team key functions look like in 2025? What new operating models are required? Does the Home Team need to change the way it is organised and the way it trains its people?

What indeed are the challenges ahead? The

Home Team planners analysed and identified four key driving forces that would shape and set the impetus for the transformation. In a future of higher load and lower manning, the Home Team would either need to transform, or “M.E.L.T”.

A More Complex Environment

The Home Team’s operating environment over the next ten years will become very different and even more complex than it is today. The decline in birth rates and ageing population has and will continue to impose significant manpower constraints on the Home Team. At the same time, departments can expect rising workload, higher public expectations, and new threats posed by terrorism and cyber-attacks. While technology may

bring about new threats, some of the new technological developments are potential game-changers that can change the way the Home Team operates, as well as enhance its operational effectiveness and efficiency.

Growing Workload

The Home Team's workload is rapidly rising. Emergency Medical Service calls have increased by about 5 percent annually over the past five years. Likewise, traveller and cargo volumes are growing. In 2015, the land checkpoints handled close to 400,000 travellers per day. With the new Changi Terminals 4 and 5, the High-Speed Rail and the Rapid Transit System coming on-stream, the volume of travellers is expected to double towards 2030. But the number of young Singaporeans entering the workforce each year will shrink due to the falling birth rates. The Home Team will face manpower constraints. The Home Team cannot handle the future load and stay effective if it operates the same way as today.

Evolving Threats

The terrorist threat Singapore faces today is at its highest level since the Jemaah Islamiyah arrests in 2001, and will likely remain so in the years ahead. The democratisation of terrorism has inspired attacks that are difficult to pre-empt or prevent. The threat of terrorist attacks using Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) means is also increasing. Besides terrorism, the nature of crime will be increasingly complex. Cybercrimes, such as online scams, have increased sharply over the years. Cyberspace has also facilitated transnational crimes, with perpetrators in overseas jurisdictions, making it challenging for the Home Team to deal with them.

Technological Advancement

In the next ten years, there will be rapid advances in technology. Some of the new developments, such as automation, data and video analytics, biometrics and artificial intelligence, are potential game-changers. The Home Team needs to ride the wave of technological developments or risk being left behind.

Rising Public Expectations

Public expectations and the demands placed on the Home Team have been growing in recent years, and can be expected to continue to grow. Citizens are now more affluent and educated, and require a more delicate approach when being engaged. The Home Team will need to constantly improve its service standards and engage citizens in a more sophisticated manner.

“ What will policing and other Home Team key functions look like in 2025? How will we make the journey there? These are the questions we are answering as part of the Home Team Transformation 2025. The answers will be contained in the new capabilities we need to build, the new ways of operating, new approaches to tackling new and evolving challenges, reaping the full potential of new technologies, better integration across the Home Team, and even changing the way we are organised, the jobs we do and the skills we need. ”

– PS Leo Yip
Home Team Transformation
e-bulletin, Nov 2016

Developing New Operating Models

The Home Team will need to transform its traditional operating models of Policing, Emergency Response, Corrections, Drug Control and Checkpoint Security. The new frontline operating models being developed will embrace these themes:

- Joint Capabilities as One Home Team
- Tiered and Differentiated Approaches
- Harnessing the power of technology
- Empowering the community; and
- Developing Next-Gen Home Team Officers

Joint Capabilities as One Home Team

The Home Team will develop joint capabilities and synergise key areas of operations to harness the strengths of the Home Team Departments (HTDs) as One Home Team. Given the increasingly complex operating environment, there is a possibility of greater occurrences of fast-burn, fast-scale incidents that necessitate rapid, often multi-HTD responses. To address this, the Home Team will take a more integrated, co-ordinated approach in how HTDs conduct operations, intelligence, and investigation to strengthen operational effectiveness. One example of a joint capability is how Joint Operations will be enhanced with clearer planning processes and integrated structures. This will enable the Home Team to deploy the most appropriate Home Team resources in handling incidents, and to facilitate more co-ordinated ground action. A new Home Team Operations Centre will be set up. It will be an integrated 24/7 co-ordination hub for managing and monitoring Home Team operations ranging from daily incidents to major crises. Analytics will be harnessed to further sharpen the common situation picture obtained. Crowd analytics and predictive modelling will be used to

inform advance deployment of HTD forces to respond rapidly to incidents.

Tiered and Differentiated Approaches

In Policing and Emergency Medical Response, the types or levels of resources deployed will be calibrated according to the nature and severity of incidents. HTDs will also anticipate where resources may be needed and deploy them in advance for a faster response. For Corrections and Drug Control, through the use of business analytics, rehabilitation and supervision regimes will be more customised based on inmates' and drug supervisees' needs and risk levels. For Checkpoint Security, a distributed clearance model will be adopted where visitors to Singapore will be cleared based on their risk profile. Those with low risk profiles can go through automated clearance channels to reduce the load on immigration officers.

Harnessing the power of technology

The Home Team will leverage technology as a key force multiplier, particularly in the areas of data analytics and automation. Data will be collated from multiple HTD sources, and analysed to improve situational awareness for better decision-making for the Singapore Police Force (SPF), an integrated and networked command harnessing data from multiple surveillance sources will provide officers with a timely and comprehensive view of potential threats and criminal activities. Immigration & Checkpoints Authority (ICA) will harvest information from its service centres, inland enforcement and checkpoints, via its next generation data platform, to enhance its situational awareness. Technologies such as automation and facial recognition will be used extensively in the Singapore Prison Service's transformed Housing Unit and the Central Narcotics

Bureau's (CNB) next-generation reporting centres to reduce manual tasks, thus freeing up officers' time for higher value work.

Empowering the community

The Home Team will take a more targeted approach to community engagement, and leverage new platforms to connect with, empower and organise the community to contribute towards the Home Team's mission. A Home Team-wide Volunteers Mobile Application is being built to help HTDs engage volunteers in the community, organise and mobilise them. Police will expand its online influence by engaging more proactively and directly with the online community. The Singapore Civil Defence Force (SCDF) will extend the reach and effectiveness of its outreach through the enhanced Community Emergency Preparedness Programme. And CNB will expand and strengthen its advocacy and network with different community groups in its fight to keep drugs off the streets. All these will strengthen the national movement of SGSecure to protect Singapore from a terrorist attack.

Developing Next-Gen Home Team Officers

Even as Home Team Transformation 2025 places more emphasis on new ways of operating and a greater adoption of technology, the Home Team needs to ensure that its people continue to be ready to support its mission of keeping Singapore safe and secure. To develop the next generation Home Team workforce, Home Team planners are reviewing how the workforce should be structured and sized in the most optimal way, refining the roles and skillsets that officers will need in future. Most importantly, the Home Team is changing the way it trains its officers. Given the changes expected in Home Team Transformation 2025, training will be

integral to equipping Home Team officers with the relevant skills and competencies to perform their new roles and duties effectively. Training curriculum will be strengthened to ensure relevance and learning effectiveness. Training will be brought to the frontline, with the development of a mobile simulation platform for officers to undergo virtual scenario-based training at the workplace. Officers will also be empowered to learn on-the-go through the development of a new training-and-learning application that allows them to access and download training materials onto their personal mobile devices.

Managing Change through Strategic Workforce Planning

The HTT2025 is a massive undertaking that requires more than a shift in resources. Driving change in an organisation as large as the Home Team is not easy; effective change management will be important. The human element - buy-in of leaders and officers at every level of the organisation, is at the heart of any successful transformation. Often, this is also the most challenging aspect to manage. Management needs to engage officers in a sustained manner, explain to them the impetus for change, and show them the potential that the transformation holds for the Home Team. Leaders need to listen and address the concerns of their people, and support them in coping with the changes.

Strategic workforce planning is a key enabler to align the development and optimisation of workforce capabilities with the organisation's strategy. In several global organisations such as IBM, Hewlett Packard, and HCL Technologies, and government agencies such as Toronto Police Service, Police Federation of England & Wales, British West-Midlands Police, Federal Bureau of Investigations in the US and Australia's New South Wales Police

Force, strategic workforce planning has been instrumental to organisational leaders in effectively transforming their organisations' business models, and empowering them to make better decisions about how they manage and develop their workforce to meet future organisational goals (Young, 2006).

The Ministry's Human Resource Division (HRD) spearheaded the Ministry's strategic workforce planning initiative and set up joint Strategic Workforce Planning (SWP) workgroups at each of the Departments in end 2015 to determine the workforce implications of the transformation plans and develop a workforce strategy blueprint that will enable the Home Team to develop a workforce well-poised to realise the Home Team's transformation plans.

Determining the Home Team Workforce of the Future

What is the structure, capabilities and size (including workforce mix) that the Home Team will need in 2025 to manage future challenges and achieve desired organisational outcomes? Development of strategic workforce plans require joint commitment and collaboration between Ministry Headquarters and HTDs as the plans need to address the unique workforce requirements of each department and be in alignment with Ministry-wide strategic directions. The joint SWP in each department distilled the workforce implications of the respective department's transformation plan and took into consideration the external and internal driving forces and constraints (including manpower trends and shifts), in order to develop a set of workforce strategies and plans to bridge workforce gaps and achieve the workforce needed in 2025.

For example, there is a projected 65 percent

increase in the demand for emergency medical services between 2015 and 2025 due to Singapore's ageing population. Emergency medical calls are projected to increase from approximately 165,000 calls in 2015 to 290,000 calls in 2025. It is thus essential for the SCDF to fully understand the impact of this trend on its workforce and identify appropriate strategies – both operational and workforce strategies – to deal with this foreseeable future demand. Clarity of the future workforce implications arising from its enhanced or new operating concepts will then enable SCDF to put in place initiatives that will facilitate the internal redeployment of its workforce to areas in demand through re-skilling and retraining.

Reskilling and Retraining - A Priority

The reskilling, retraining and development of the Home Team workforce is a priority as it is the key to successful transformation. Reskilling will enable officers to take on higher value work progressively and competently when new concepts of operations are introduced and existing jobs are re-designed to leverage new equipment and technologies.

For example, SPF frontline officers will need to be trained to use pistols which will replace their revolvers while Police Coast Guard officers will need to be trained in counter-assault skills and use of sub-machine guns and carbines so that they will be able to respond to terrorist attacks and other threats in Singapore waters. Beyond new equipment, as the Home Team leverages analytics and data, officers will also need to be trained to handle, synthesise and sense-make large amounts of information. Increasing automation of tasks will also free up officers from routine tasks for higher value-added work, such as sharpening profiling and first response capabilities for ICA officers.

To identify the new skillsets that Home Team officers need in order to progressively implement new concepts of operations over the immediate one to two years, a Skills Transformation and Development Taskforce comprising members from across the Home Team Departments was set up. The Taskforce was also given the mandate to identify training gaps and propose approaches to train officers in key skills identified.

The Home Team will subsequently translate the Taskforce's recommendations into appropriate training programmes for Home Team officers. As the Corporate University for the Home Team, the Home Team Academy (HTA) is also partnering established institutes of higher learning to provide customised pathways for Home Team officers to obtain academic and professional qualifications, as part of efforts to encourage personal development and upgrading.

The Home Team is also investing significant resources to enhancing its training facilities and leveraging new training delivery methods to bring effective, bite-sized learning programmes closer to officers. Over the next few years, the training facilities at the Civil Defence Academy will also be revamped to give SCDF officers enhanced and more realistic training. This will help to improve their response capabilities to different types of emergency situations on the ground.

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 the strategic stakeholders such as local communities, businesses and international partners. The future Home Team officer needs to be adaptable and resilient to maintain a high state of readiness and to effectively tackle

new challenges.

Capturing Hearts and Minds

The readiness of the different groups of Home Team officers to embrace the changes and prepare themselves for new challenges is paramount to whether the Home Team can effectively roll out its transformation plans, including reskilling and retraining officers to achieve desired outcomes.

To this effect, Home Team leaders started a transformation change management effort two years ago to help Home Team officers at all levels - from the leadership group, middle managers to the last man on the ground - appreciate and understand the impetus and need for the Home Team to transform. Several avenues such as townhall sessions and focus group discussions (led by the Home Team's top leadership) were conducted to engage and keep every officer across the Home Team informed of the transformation effort. These sessions also served to excite and involve Home Team officers in the transformation journey by providing opportunities for officers to share their concerns, provide feedback on future organisational capabilities and skills as well as to co-create the desired future.

These engagement sessions were complemented by the dissemination of materials such as slides, digital infographics, videos and FAQs through multiple platforms (emails, intranet and hardcopy). Besides serving as handy references for officers, these materials also facilitated communication with officers who were not able to attend the briefing sessions. Officers were also actively engaged in different work streams of HTT2025 initiatives such as project teams or as facilitators of engagement sessions, so that they became fully aware of the new skill requirements for

Frontline Operating Models of 2025

Policing

Dynamic Incident Response Integrated & Networked Command Tiered & Differentiated Investigations



Emergency Response

Tiered Approach Dynamic Resource Deployment Partnering Community



Corrections

Differentiated Intel-driven Regimes Transformed Housing Units Life cycle approach to manage offenders



Drug Control

Intel-based Enforcement Targeted Preventive Drug Education Customised Supervision Regimes



Checkpoint Security

Secured Automated Clearances as the Norm Differentiated Clearance Approach Service Centre Next-Gen: Self-Service as the Norm



their areas of work and the need for up-skilling to remain relevant in their future roles. Some useful ideas that transpired from the discussions included the need to preserve the ‘human touch’ and ‘ground instincts’ even as we leverage technology, and the need to ring-fence time for training.

The Home Team is also nurturing a One Home Team mind-set to further strengthen close collaboration within the Home Team. New milestone courses are being developed to address developmental needs of officers at key points of their careers. These courses will not only allow our officers to deepen their understanding of the Home Team and develop a Home Team perspective, they will also provide them with the opportunity to bond with fellow officers from other HTDs, form new networks and develop a One Home Team mindset through shared experiences.

Are We Ready?

Clear transformation plans have been developed but the question remains: Is the Home Team ready for the future?

The key will be the timely and robust implementation of the transformation initiatives and their integration across the Home Team in the coming years. Even as the Home Team manages the current high tempo of operations, it has to continue driving the implementation momentum, for HTT2025 is a massive undertaking that requires more than a shift in resources. Success will require deep transformation of the Home Team’s modus operandi as well as the buy-in of leaders and officers at every level of the organisation.

Indeed, close partnership and commitment is required from all stakeholders – senior management, middle management and indi-

“ *Home Team Transformation 2025 is a critical exercise for all of us. It is to enable us to achieve a quantum leap in preparation and capability building for a more complex, more unpredictable and faster-paced future, and where the expectations on our shoulders to keep Singapore safe and secure, have never been higher.*

It sounds daunting, but seen another way, our ‘transformation’ is just an extension of what we are already doing every day – see how our operating environment is changing, assess the resources available, and the new tools that have become available, and adapt ourselves accordingly so that we are able to carry out our mission even more efficiently and effectively. I look forward to continuing this journey with you. ”

– PS Pang Kin Keong
September 2017

vidual officers. Everyone needs to embrace a progressive outlook and be prepared to learn new skills, acquire new knowledge and undertake new roles. As officers take on new challenges and responsibilities with courage and determination, the Ministry of Home Affairs stands committed to investing in the re-skilling, training and development of officers, so that they are equipped with the right skills, knowledge and capabilities to contribute meaningfully to the Home Team mission of keeping Singapore safe and secure now and in the future.

About the Authors



(From left to right) Ms Jill Tan, Senior Executive, Strategic HR Workforce, HRD; Ms Shirlyn Ng, Senior Director, Human Resource Division; Mr Jason Chen, Senior Director, Planning & Organisation Division; Mr Mirza Saad, Assistant Director (Strategic Planning, Innovation), P&O; Ms Christi Lau, Senior Assistant Director (HR Planning), HRD; and Ms Ng Huey Ling, Deputy Director, Strategic HR Workforce, HRD.

The team would like to thank Ms Amanda Chua (Deputy Director, HT Training & Learning/Skills Transformation), and Ms Teresa Cheong (Assistant Director, Strategic HR Workforce/Safety & Security) for their contributions to the article.



Human Resource Division, Ministry of Home Affairs

To develop a workforce well-poised to implement and realise the Home Team's transformation plans, Human Resource Division of the Ministry Headquarters has formed teams to look into three areas: (i) Strategic workforce planning; (ii) Skills transformation and development; and (iii) Nurturing a One Home Team mindset in officers to strengthen collaboration and adaptability to change.

HRD has worked closely with strategic partners in the Ministry Headquarters and the various HTDs to actively engage and involve Home Team officers in the development of the various blueprints and implementation of the plans that are ready.

The cooperation, dedication and perseverance of the various stakeholders across the Home Team were instrumental in ensuring the steady progress made on all fronts to prepare the Home Team officers for future demands and challenges. This is an ongoing journey. HRD will continue to partner our stakeholders to champion effective people strategies, delivery people-centric services and foster a culture of excellence for one Home Team.



Planning & Organisation Division, Ministry of Home Affairs

To inspire and partner Home Team agencies to create the future for MHA, the Planning & Organisation Division (P&O) prepares MHA by ensuring that our strategic plans are informed by a comprehensive analysis of challenges, opportunities and priorities. The Strategic Planning (SP) Directorate leads in strategic and corporate planning for MHA. The directorate articulates the Home Team's strategic priorities to provide direction for Home Team organisational and resource outcomes.

SP Directorate is also responsible for driving Home Team Transformation. The directorate rigorously reviews the various Home Team agencies' and Staff plans to ensure they are on track, and implements timely adjustments where needed. SP Directorate is responsible for formulating the Home Team's change management strategies to sustain momentum in HTT2025. It is critical to maintain effective communication channels with officers to continue seeding and amplifying the Transformation message.

References

Young, Marry. B. (2006). *Strategic workforce planning: Forecasting human capital needs to execute business strategy*. New York, NY: Conference Board.

Nayar, Vineet. (2010, June). A Maverick CEO Explains How He Persuaded His Team to Leap into the Future: How I Did It. *Harvard Business Review*, 1-5.

HARNESSING THE POWER OF TECHNOLOGY

Use of Artificial Intelligence in the Home Team

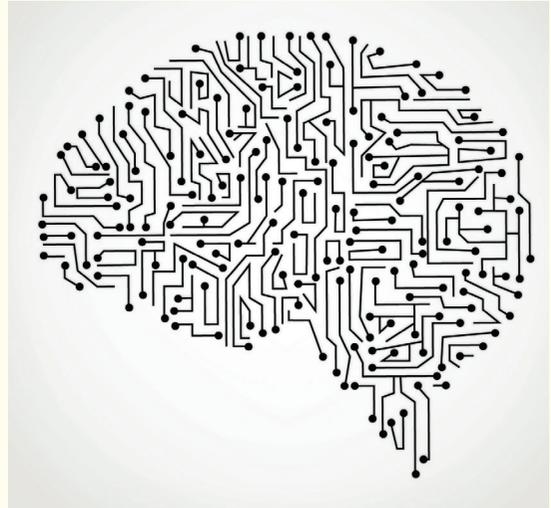
By Dr. Jonathan Pan, Office of Chief Science & Technology Officer,
Ministry of Home Affairs,
and Centre for Cyber Security Studies, Institute of Safety and Security Studies

Grace Koh

Centre for Cyber Security Studies, Institute of Safety and Security Studies

What the Home Team needs

As the Home Team advances full steam towards Transformation 2025, technology will be a key enabler. By 2025, the Home Team intends to become significantly more data-driven with the deployment of nation-wide sensors like closed circuit television, live feeds and police cameras to reduce the time needed to assess incidents and make timely decisions to respond optimally. These sensors produce massive amount of data and will need to be processed and analysed to provide relevant insights that will facilitate decision-making for Home Team officers. Security alerts generated from each of these sensors deployed will need to be analysed and possibly investigated. According to a Damballa analysis that studied the adoption of technology in the US, a significant portion of alerts generated by such technology devices were false (Moore, 2016). Putting it in Singapore's context, as Singapore becomes more connected, coupled with the strong collective adoption of smart technologies, we too will have lots more generated alerts, including those related to se-



curity, to manage. Manual analysis of such alerts will be a strenuous and labour intensive activity. The manpower needed to perform such analysis will not be easily available. The hope therefore is that Artificial Intelligence (AI) will meet this need, as automated and autonomous tools to support homeland security efforts.

Mr K Shanmugam, Minister for Home Affairs and Law, highlighted the importance of AI at the 2017 Millipol conference when he said: “Having thousands and thousands of cameras is one thing; what’s required is making them smart, making them fused, bringing the data together and having the artificial intelligence to analyse and, in fact, predict behaviour. We cannot just wait for something to happen but must be able to predict that when a certain pattern develops, we know what’s going to happen. That’s going to be critical – unusual activity being flagged out in real time, aided by facial recognition, and a whole variety of technologies.”

Examples of AI

AI is defined as intelligence exhibited by computers. It is software that mimics the functions and abilities of the human brain, including the ability to recognise something that is of interest, engage in conversation, and intelligently control an autonomous vehicle. One of the functions of the human brain that AI attempts to mimic is the ability to learn new skills or undertake new tasks. Learning may be done through the feeding of data. This ushers in the popularly known technology, Machine Learning, a form of AI that involves shaping the machine learning software through feeding it with large amounts of data. The machine learning software learns by itself from the data without any need to have someone program its functionality. There have been many recent successes with machine learning solutions due to the rich availability of data from the Internet and advances in high computing capabilities of computers.

AI is increasingly playing a bigger role in everyday life. For example, intelligent virtual assistants like Apple’s Siri understand human language and can perform simple tasks like searching for current weather forecasts.

Netflix is using AI to “train” its technology to provide better viewing recommendations by feeding it with massive amounts of information. Earlier this year, we witnessed the AI algorithm Libratus from Carnegie Mellon University win its first poker world competition and Google’s DeepMind AI, AlphaGo, defeating both Go Champions Lee Sedol and Ke Jie. (Go, being an abstract strategy board game invented 2,500 years ago, where two players compete to acquire territory, had been considered one of the toughest games for AI.) AlphaGo’s and Libratus’s victories over the reigning human champions were testament to the exponential rate at which AI has advanced.

Aside from its achievements in the gaming arena, AI’s advancements have also seen it being developed and implemented in self-driving cars. More than 10 million vehicles will be deployed, with some self-driving features, onto the roads by 2020. The United States Department of Defence’s (DoD) R&D division is also working to develop autonomous fighter planes that are capable of performing complex dogfighting stunts, controlled solely by AI.

AI Applications in Safety and Security

In the context of safety and security applications, AI has had a long history of being an integral part of solution deployment. Consider the Automated Biometric and Behavioural Screening Suite (ABBSS) used by the Immigration & Checkpoints Authority (ICA), which encompasses a state-of-the-art video analytics system and can perform real-time facial recognition and cross-referencing against a database. ABBSS can search recorded footage based on multiple parameters, such as colour, size, number plate, speed and direction of the moving object. The system has been deployed at the Woodlands Check-

point and has enabled ICA to identify many blacklisted travellers. It has boosted the efficiency and effectiveness of our border security operations (Shanmugam, 2017).

And predictions are becoming more accurate too. The United States Department of Homeland Security (DHS), with the Kaggle data science community, is hosting a data science contest to build algorithms that can automatically predict locations of concealed items with checkpoint body scanners. Acquired by Google this year, Kaggle built its reputation on hosting online competitions where data scientists compete for money by developing approaches to complex machine learning algorithms.

The possibilities are seemingly endless. Police in Durham will be using AI to help officers decide if a suspect should be kept in custody or released on bail. The programme, HART (Harm Assessment Risk Tool), was trained on 5 years' of offending histories data, between 2008 and 2012. It also looks at a suspect's gender and postcode to assess how risky it is to release the suspect.

Google is reportedly using a combination of AI and humans to identify and remove extremist videos from YouTube. Over 6 months or so, Google has relied on video analysis models to search for and assess more than 50 percent of terrorism-related contents. It created more "content classifiers" to enable automated machines to better identify and determine which contents are extremist. The human input came from 50 NGOs which were given grants to assist in identifying the types of content.

AI has also been instrumental in the development of technology to help victims of child exploitation. These solutions focus on quickly identifying materials featuring victims of

child exploitation, as well as their perpetrators, on both the open and dark web. Every day, more than 100,000 escort ads are posted in the United States, alone, according to the Thorn website (www.wearethorn.org). Included amongst them are ads for children who are being sexually exploited. Given limited resources, to have law enforcement agencies manually go through and assess the ads is an almost impossible task.

Thorn, a non-profit technological task force organisation, leverages on AI to quickly sift through these ads daily and identify the ones with the highest risk profiles. Its algorithm correlates data from information that is publicly available and presents the data to a member of the task force, who verifies each point of data to ultimately identify victims and perpetrators. The group has managed to identify 6,000 victims and helped reduce law enforcement investigation time by more than 60 percent (Thorn, 2017). Thorn is now working to develop solutions for the dark web where 2 – 3 percent of the sites promote child sexual activity. The dark web has traditionally been a challenging terrain for law enforcement agencies as it enables anonymous online communication. Websites are not searchable or reliable – new sites come up and go down as and when the hosts wish, leaving no digital footprints. Materials thus need to be downloaded within a short period. Although they take up only a small proportion of known sites, child sex sites account for about 80 percent of the dark web's traffic. These sites carry hundreds of thousands of images and videos of children being exploited (Pitkow, 2017).

Thorn is now working to incorporate AI in their solutions for the dark web that will be used to detect new sites, collect and prioritise information, and correlate disparate data by integrating identification tools such as facial recognition. The solution will be tested out in

eight countries with agencies that specialise in dark web child exploitation investigations.

Key Considerations in Use of AI

Automation

With many technologies being deployed by the Home Team, AI could be used to deal with the associated challenge of information overload and to augment the decision-making and sense-making capabilities of Home Team officers. AI could be deployed to perform the unglamorous task of analysing massive amounts of data or sensor feeds and providing human operators or ground officers with summarised and salient points. For example, all CCTV footages could be monitored by machines powered by AI, which will alert the operator when anomalies occur like fire or sound of explosions.

AI could be used to discover and identify new issues or problems before it happens. For example, the US Defense Advanced Research Projects Agency (DARPA) created the Cyber Grand Challenge, an international competition for academics and researchers to develop advanced autonomous systems that could detect, assess and patch system vulnerabilities, in order to correct software flaws in real-time. In addition to patching vulnerabilities, competing teams were also encouraged to search for weaknesses and gaps within the codes of their opponents, and exploit them before they could be patched. While the intention of the game was to help cybersecurity professionals, it was clear that machines and AI could be leveraged for defence and attacks.

Competency Retention

Besides using AI to perform and automate routine and dull tasks, AI can be deployed to address the Home Team's need to retain ex-

pertise and experience. This can be achieved by having experienced and skilled officers train the AI software on a regular basis. In 2016, the Massachusetts Institute of Technology (MIT) published its work on developing an AI software that is able to learn from cyber security operators to differentiate between security events that were malicious and which required further investigation and those that were not. There was no formal programming; the software learnt on a daily basis by observing how skilled and experienced operators made their decision choices. The software progressively acquired the 'expertise' and attained matching competencies in identifying malicious activities. The potential benefits of such trained AI software is that the experience and knowledge is 'copied' and 'retained'.

However, AI also has limitations with grave implications when misused.

Adversarial Use

Just as AI can potentially provide the Home Team with needed advantages, there is a downside to this technology; it is similarly available to adversarial and criminal elements, who can use the same technology solutions to perform complex attacks against Singapore and evade detection. Google recently developed a speech synthesis AI software that converts text to speech and sounds more like a regular human than computer synthesised speech. When this solution is perfected, it could deceive law enforcement officers into thinking that they are speaking to a person rather than a software.

In one of the last interviews that former United States President Barack Obama gave before stepping down, he voiced great concern about AI. He told Wired magazine that his greatest fear from AI is not about robots controlling the world as seen in the movie 'Ter-

minator’, but that AI could be used to identify vulnerabilities and exploited to attack critical systems.

Mis-trained

AI could be led astray by the data used to train it. In 2016, Microsoft released a Twitter bot (or a software robot) named Tay to pick up conversational cues and engage with humans on the Twitter platform. The more Tay chatted on Twitter, the smarter it would become. However less than 24 hours after its release, Tay started tweeting all sorts of misogynistic and racist remarks largely in response to the people who were tweeting at it. Tay was immediately taken offline by Microsoft following an outcry by the social media community.

Cyber Security Risks

Another risk that AI poses is from its own cybersecurity risk. As with all software, AI is also susceptible to cybersecurity attacks. Apart from the conventional cyber-attack techniques, there are forms of attack patterns unique to AI software. One is to exploit an AI model trained to operate in a specific manner by undermining or stopping its proper functioning. For example, an autonomous patrol robot can be forced from performing its patrol task by placing a ‘stop’ sign in front of its visual sensor. Another method is to maliciously ‘poison’ the training dataset used to develop the AI software to create intended blind spots so that it is unable to recognise its intended target, leading to false negative detections.

Loss of Jobs versus New Roles

Some have cautioned that as AI advances and takes on more roles, there will be a loss of jobs. However, there are others who argue that the benefits outweigh the losses. For

the Home Team, the benefits of adopting AI means it can keep pace with evolving threats amid a changing environment. Indeed, even as some jobs are lost, new ones have to be created with the adoption of AI. The new roles include those of AI or Machine Learning engineers and project managers to deploy and maintain AI deployments, and AI validators to verify and validate AI deployments and to upkeep its accuracy and operational effectiveness. New posts will also have to be created to ensure that AI behaves legally, ethically and in a non-discriminatory manner. Cybersecurity expertise will be needed to protect AI platforms from cyber-attacks.

Conclusion

Artificial Intelligence has advanced significantly in recent years. There have been many reported outstanding performances achieved by AI developers. It is now the technology buzz word in the industry and in academia. However, as with all technologies, there are limitations and associated risks. Also there are naysayers who fear the future filled with AI.

For the Home Team, such advancements offer many Ops-Tech opportunities to enhance the Home Team’s capabilities and support its transformation endeavour. The adoption of AI into the homeland security environment around the world is, however, still in its early stages. The Home Team will need to strategise on this technology adoption and develop Concepts of Operations (CONOPS) around it to harness its ‘power’ to support our endeavour to keep Singapore safe and secure.

About the Authors



Grace Koh, an Information Systems Officer, is currently with the Home Team Academy Centre for Cyber Security Studies. As part of Dr. Jonathan Pan's Strategic Initiatives team, Grace is involved in outreach efforts to Institutes of Higher Learning and in various initiatives such as bounty hunts. She is interested in many areas of cybersecurity such as societal, psychological, artificial intelligence, autonomous vehicles and international governance.

Honouring our Expert: Dr. Jonathan Pan



Dr. Jonathan Pan is the Director of Automation and Robotics in the Office of Chief Science & Technology Officer, Ministry of Home Affairs Headquarters. He is concurrently the Director of Strategic Initiatives at the Centre for Cyber Security Studies (CCSS), one of the specialist centres of the Institute of Safety and Security Studies. His key contributions are in cybersecurity and artificial intelligence, where he is a pioneer in developing innovative tools such as simplifying the analysis of computer viruses for cyber investigators. He is currently leading the development of capabilities using drones, intelligent sense-making systems and intelligent virtual assistants to improve operations. Prior to OCSTO and CCSS, he was

with the Technology Futures Directorate of the Ops-Tech Group (OTG), Ministry of Home Affairs Headquarters where he was deeply involved in the trial and experimentation of new technologies with Home Team Departments (HTDs).

Dr. Pan, who has a doctoral degree in the study of malware, is an adjunct lecturer with Nanyang Technological University where he teaches Cyber Security and Artificial Intelligence to post-graduate students. He has published numerous cybersecurity papers in peer reviewed journals. He also volunteers with the Singapore Police Force as an Honorary Volunteer Special Constabulary (Specialist) in the area of cyber security and cybercrime.

In recognition of Dr. Pan's outstanding achievements and contributions, he was awarded the 2017 Science & Technology Excellence Award, Ops-Tech/ Engineering (Individual) category.

References

- Baraniuk, Chris. (2017, May 10). Durham Police AI to Help with Custody Decisions. *BBC News*. Retrieved from <http://www.bbc.com/news/technology-39857645>
- Chen, Stephen. (2017, June 29). Inside the AI Revolution that's Reshaping Chinese Society. *South China Morning Post*. Retrieved from <http://www.scmp.com/news/china/society/article/2100427/chinas-ai-revolution-and-how-its-rivalling-us>
- Lee, Kai-Fu. (2017, June 24). The Real Threat of Artificial Intelligence. *New York Times*. Retrieved from <https://www.nytimes.com/2017/06/24/opinion/sunday/artificial-intelligence-economic-inequality.html>
- McMillan, Robert. (2015, January 16). AI has arrived, and that really Worries the World's Brightest Minds. *Wired* magazine. Retrieved from <https://www.wired.com/2015/01/ai-arrived-really-worries-worlds-brightest-minds/>
- Moore, Keith. (2016). The Race against Cyber Crime is Lost without Artificial Intelligence. *ISSA Journal*, 14(11), 27-34.
- Pitkow, Jim. (2017). Child Sexual Abuse Thrives in the Darkest Parts of the Internet. *Global Perspectives from Experts at INTERPOL World 2017 Congress*, 41-42.
- Ranganath, Kris. (2017). As Smart Cities Transform, Safety and Security Come First. *Global Perspectives from Experts at INTERPOL World 2017 Congress*, 119-121.
- Savvides, Nick. (2017). Outsmarting Intelligent Cyber Security Threats with Machine Learning. *Global Perspectives from Experts at INTERPOL World 2017 Congress*, 57-59.
- Shanmugam, K. (2017, July 17). Speech at the Home Team Science & Technology Exhibition & Conference for Homeland Security (SciTECHS). Retrieved from [https://www.mha.gov.sg/newsroom/speeches/Pages/The-Home-Team-Science-Technology-Exhibition-Conference-for-Homeland-Security-\(SciTECHS\)-Speech-by-Mr-K-Shanmugam,-Minis.aspx](https://www.mha.gov.sg/newsroom/speeches/Pages/The-Home-Team-Science-Technology-Exhibition-Conference-for-Homeland-Security-(SciTECHS)-Speech-by-Mr-K-Shanmugam,-Minis.aspx)
- Thorn. (2017). *Spotlight: Human Trafficking Intelligence and Leads*. Retrieved from <https://www.wereathorn.org/spotlight/>

Use of Analytics in Operations

THE SINGAPORE PRISONS' ANALYTICS JOURNEY

By Dr. Melvinder Singh and Mark Toh
Singapore Prison Service

Every correctional service aims to bring about change in the lives of the offenders they manage. Decisions made at every point in the offender's rehabilitation journey will not only affect the offender but also the lives of the people around him and society at large. Given the vast amount of data that correctional services have access to, it is useful to leverage analytics to promote deeper understanding of current reality, enable better sense-making and aid in resource allocation. Analytics – information resulting from the systematic analysis of data or statistics aids this work by supporting the decision making process. That being said, analytics form but a part of the fabric of the decision making process and should never be relied on as the sole factor in decision making.

This article discusses some of the lessons learnt from the Singapore Prison Service's (SPS) work in model development and provides some insights into the difficulties faced. The focus is on sharing aspects of the SPS journey that will be of practical value to other agencies embarking on their own analytics journey.

Modelling projects typically follow a defined sequential structure which involve acquisition and preparation of data, gaining insight

from data (i.e. creating the model), translation of data into policy, and lastly implementation and maintenance of the data model (Dean, 2014). Thoughts on each stage of the process will be provided and the article will conclude with two key lessons learnt in the course of our journey.

Finding the Data

At the heart of any attempt to build a model is an understanding of factors that are correlated with the outcome and finding data that are effective proxies for these outcomes. This is true of all outcomes regardless of whether they relate to purchasing habits or online search patterns. As such, the conceptual first step of any analytics project involves reviewing the literature to understand what others have found.

The major challenge faced when looking for such variables is accounting for cultural nuances. What is salient in one setting may not make sense when translated into a different setting. Using drug offending as an example, literature from western jurisdictions have placed less emphasis on the role of drugs in re-offending. (Andrews, Bonta & Hoge, 1990). In fact, western risk assessment tools like the Level of Service Case Management Inventory

(LSCMI) (Andrews, Bonta & Wormith, 2004) only devote a relatively small eight risk points out of 43 risk points to understanding drug and substance abuse. However, this is not the case in Singapore given our zero tolerance policy towards drugs. Any attempt to develop a risk assessment model needs to take into account such nuances, otherwise the variables used would not be an accurate representation of what is being predicted.

Knowing the Data

Having identified factors that are relevant to understanding outcomes of interest from the research literature, the next challenge is to start finding proxies for these factors. The biggest difficulty at this juncture is knowing what data is at the disposal of model developers. In order to achieve this, it is good practice to meet with data owners to understand the type of data that is available and whether this data is retrievable.

In terms of understanding the data that is available, a basic approach would involve requesting a copy of the data dictionary. A data dictionary essentially defines each and every data field available and provides information on how the information is captured and the way it is represented in the data field. Practical challenges associated with this include the fact that data dictionaries (should they exist) typically represent a description of the data that may not always be applicable in practice. The reality is that not all information captured within the data dictionary will be available to the model developer as ground users may not capture all information specified within the data dictionary. In the worst case scenario, data fields may be used to capture information that is inconsistent with the original intent of the field. To compensate for this, developers need to be careful when making assumptions about the origin of the

data and work with stakeholders who own the data to better understand potential issues with the data, including problems associated with accuracy and consistency.

Retrieving the Data

Assuming that the data exists, the next step involves the retrieval of the data. This is often easier said than done. The majority of existing Information Technology (IT) systems are often designed for data storage rather than data retrieval. While the data can often be viewed easily through user interfaces and is physically present, there is often a limited backend table structure that may add obstacles to the data retrieval process.

For example, a patient at a hospital may be identified by two unique identifiers (UID): an NRIC number for someone who is seen at the hospital outpatient clinic and a hospital admission number for someone who is admitted to hospital. In theory, these two case dockets reside within the same hospital record keeping system. However, due to the difference in unique identifiers, it may almost be technically impossible to link these two sources of information together. It is thus essential to understand the backend data architecture, as this enables developers to extract the required data in a targeted and efficient manner.

Data Integrity

Having ascertained that the data exists and can be retrieved, the next challenge that presents itself involves the cleaning and preparation of data for analysis. A data model is only as good as the data it uses. Ensuring data integrity is the most time consuming part of developing a model, and often, not enough time is catered for this task within project timelines. Ensuring data integrity is especially dif-

difficult when the information captured within each field in the database is poorly defined and equally so if the extraction process has been complicated due to poor data architecture.

Data integrity checks focus on two key areas. The first area involves ensuring that the data captured is valid. This area of verification usually involves looking for implausible scenarios like a reported age of 123 years, an NRIC number that begins with any letter other than 'S' or 'T', or simply duplicate cases. A second area of checking data integrity involves the actual verification that data fields are accurately captured. This process invariably involves cross referencing data from various sources.

An example of data irregularity would be a case in which a patient who was documented as being admitted to a hospital is also recorded as having made multiple visits to an outpatient clinic during the time he was admitted. Resolving these genre of cases tends to take a lot of time as this verification process has to be done manually for each and every case detected. This is often exacerbated by the sheer number of cases needed to build reliable models; often many inconsistent cases are also detected.

The big insight here is that there is no running away from data integrity checking in analytics. SPS managed the process through a system of logic checks which looked for inconsistencies between the data fields churned out from the data system. Inconsistencies included situations in which records clearly conflicted with each other. There are various software solutions available that can help automate part of this process of assuring data quality, but even the best software will require an understanding of the data and an ability to specify what constitutes an anomaly.

Understanding the Data

A major part of analytics involves understanding the data at hand. This involves checking the descriptive statistics to understand if each variable will be useful for differentiating between two groups of interest. What this means, for example, is that for a variable such as age to be useful in determining whether a person is going to be re-imprisoned, a difference in average age between those who are re-imprisoned and those who are not must be seen.

Understanding the data extends beyond just looking at the descriptives. The real challenge for an analytics team is to engineer the data into a sharper set of variables to secure richer insights. The usefulness of data engineering can be seen from the following example. Researchers at a hospital are trying to determine which of their patients are more likely to be readmitted into that hospital. The hospital has data on the total number of visits a person has made to the hospital in his lifetime. However, visits from twenty years ago may not be as relevant as visits made in the last five years. Hence, a new data field has to be created to capture only visits made in the last five years.

The biggest challenge faced in the understanding of data was getting people who have deep institutional knowledge to be involved in analytic work. However, many of these older officers were not confident about their ability to take on such analytical work, and hence avoided it. To compensate for this, staff involved in our modelling projects were very experienced with the processes being modelled and had a strong mathematical/statistics background to help understand the data.

Gaining Insights from the Data

In the world of modern analytics, one is spoilt for choice in terms of the software and statistical packages that can be deployed to help gain insights from the data (Smith, 2016). A temptation exists to run every possible analysis in the hope of finding a model that is of the most utility. There are several considerations that need to be weighed up in this respect. Chief among these is the aim of the model. Should absolute accuracy be paramount, techniques like neural networks (Palcosay, Wang, & Brookshire, 2000) and random forests (Breiman & Schapire, 2001) modelling exist that can allow for near perfect accuracy.

The main limitation to these techniques from a public policy perspective is that the algorithms for these models function in an almost opaque manner. The model developer will never be able to explain why an event is predicted to occur for a particular individual nor can the developer explain how each variable impacts the model. Another limitation associated with neural networks and random forests approaches is that high accuracy essentially means that the final model is customised to the sample it was developed on. In short, these models perform poorly when applied to a different sample with different characteristics, or when the sample it was developed on is subject to change.

As transparency and generalisability are paramount, a regression-based approach (Hosmer, Lemeshow & Sturdivant, 2013) was used. Regression approaches trade overall accuracy for transparency and generalisability. What this means from a layman's perspective is that one knows how the variables in the model perform and that findings can be replicated if applied to a similar sample. The trade-off to using a regression-based approach is that the

experience of the analyst plays a big role in deciding the utility of variables in the model. In simple terms, data models developed using regression-based approaches incorporate elements of 'art' along with the science.

Data into Policy

A major part of the model development process involves communicating to stakeholders how the model can be used. One cannot understate how important the stakeholder engagement process is to ensure good understanding of what the model can and cannot do. There will always be an organisational temptation to use a model beyond what it is meant to do. It is up to the analytics team to help define the limits for how the model can be applied and ensure that stakeholders know the limits of the model.

There were many valuable lessons to be learnt from the policy implementation process. The biggest lesson was that stakeholder engagement should not come after the model has been developed. Rather, stakeholder engagement should be an ongoing process starting from conceptualisation, so as to ensure better understand how a particular model fits into the existing policy frameworks. In this regard, SPS now has a policy of engaging stakeholders from the point where the model is first requested to better understand stakeholder needs and to ensure that there is buy-in to implement the model once it is completed.

Another key lesson learnt by SPS is that when making decisions based on our models, what is statistically optimum may not be practically desirable. What is practically desirable is often circumscribed by resource constraints. To this end, it is crucial to explain to stakeholders what the trade-offs are and what each of these trade-offs mean for policy.

Implementation and Maintenance

Implementation of models was challenging as SPS did not have an enterprise system suited for the implementation of these models. In order to overcome this, SPS implemented the model via an Extract Transform and Load (ETL) which allows for an external system to perform the necessary calculations before returning the calculated score back to the host system for display.

An inherent problem associated with the ETL approach is that the data pathways need to be clearly mapped out in order for the tool to be successfully implemented. A good data dictionary is key to ensuring successful implementation. This dictionary should clearly document where the raw data is drawn from and provide clear instructions for how data engineered variables are transformed.

The analytics team also needs to be ready to provide support in terms of validating the model after the ETL tool has been completed. This involves doing a check to ensure that the tool is scoring the model correctly and, importantly, ensuring that any issues are ironed out prior to deployment. SPS found the implementation process particularly insightful as it allowed the team to gain an in-depth understanding into the actual database layout. Insights gleaned from the implementation of models have proven invaluable to subsequent model development efforts as it allowed SPS to better understand the limits of the data.

The priority for models developed by SPS is transparency and robustness. A model maintenance framework serves to support this imperative for robustness. The SPS model maintenance framework centres round a yearly check to ensure that the model is still useful and limits the lifespan of a deployed model to five years from development. At the

five-year point, a model redevelopment process is undertaken which involves rebuilding the model with new data. Having a model life-cycle of five years is crucial as it establishes a discipline for the analyst to consider new information. This model lifecycle is especially crucial given the rapid improvements in data capture which leads to new information being captured with higher fidelity than previously possible.

Two Key Lessons

Having reflected on the SPS journey, two things stand out as being crucial in order to successfully build good models: good data and, as importantly, good people.

For any agency that wishes to embark on the data analytics journey, good data governance is vital. One must understand what the data means, where it comes from, and the limits of the data in terms of accuracy and consistency. Only then will we have confidence in the models we build.

Having the right people is also key to a good analytics team. While this seems an obvious statement, it is difficult to achieve. The right people are those that possess a serendipitous mixture of technical competency, good insights into the nature of the agency's work, and the passion to build models that effect positive and practical change.

Analytics has the potential to help the Home Team right size resource allocation and achieve its operational objectives. It is hoped that the points shared in this article will encourage others to experiment with analytics to see how it can help form part of the existing decision making frameworks, to enhance their day-to-day operations.

About the Authors



Dr. Melvinder Singh is a clinical psychologist by training and has been with the Singapore Prison Service for 16 years. During this time, he has served in variety of leadership positions within SPS in the areas of both research and programme evaluation. Melvinder is currently the Senior Assistant Director of the Data Science Branch in the Singapore Prison Service. In this role, he shapes the strategic direction of Data Analytics in SPS. He also advises SPS management on a variety of data related issues associated with data management reporting, the use of analytics and the optimisation of SPS business processes.



Mark Toh is currently an assistant director with the Data Science Branch at Singapore Prison Service. He has played a major role in the development of the analytics systems used by SPS. Moving forward, Mark is involved in the development of risk screening tools related to specific offending outcomes like drug and violence. He is also currently exploring the utility of automating mechanical processes within SPS to help optimise the allocation of resources.

References

- Andrews, D., Bonta, J., & Hoge, R. (1990). Classification for Effective Rehabilitation: Rediscovering Psychology. *Criminal Justice and Behavior*, 17, 19-51.
- Andrews, D., Bonta, J., & Wormith, J. (2004). *The Level of Service/Case Management Inventory*. Toronto, Canada: Multi-Health Systems.
- Breiman, L., & Schapire, E. (2001). *Random Forests*. *Machine Learning*, 45, 5-32.
- Dean, J. (2014). *Big Data, Data Mining and Machine Learning: Value Creation for Business Leaders and Practitioners*. Hoboken, NJ: John Wiley & Sons, Inc.
- Hosmer, D., Lemeshow, S., & Sturdivant, R. (2013). *Applied Logistic Regression, Third Edition*. Hoboken, NJ: John Wiley & Sons, Inc.
- Palcosay, S., Wang, P., & Brookshire, R. (2000). Predicting criminal recidivism using neural networks. *Socio-Economic Planning Sciences*, 34, 271-284.
- Smith, J. (2016). *Data Analytics: What Every Business Must Know About Big Data And Data Science*. Pinnacle Publishers, LLC.

Use of Virtual Reality Technology in Training

IN CONVERSATION WITH DR NARESH KUMAR
DIRECTOR, OFFICE OF THE CHIEF SCIENCE &
TECHNOLOGY OFFICER & HUMAN FACTORS

By Shazwani Babjee

Home Team Training & Learning Office, Home Team Academy

Dr. Naresh Kumar joined the Office of Chief Science & Technology Officer in the Ministry of Home Affairs in 2007. He has since been instrumental in introducing to the Home Team human factors engineering, which is the science of applying knowledge about human abilities, limitations and other relevant human characteristics to the design of systems, machines, tasks and environments so that they are safe, comfortable and effective for human use. He has delivered solutions for the Home Team in the areas of ergonomics, human performance, profiling and screening, smart surveillance and visual analytics, and worked closely with various Home Team Departments on human systems integration in Command and Control (C2) platforms, robotics and automation, and Virtual Reality (VR). In 2016, Dr. Naresh and his team set up the Human Performance Centre, a state-of-the-art human factors facility that seeks to optimise work

processes, operational systems, and the performance of Home Team officers. Dr. Naresh was conferred the Innovation & Development (Individual) Award at the inaugural Home Team Science and Technology Excellence Awards ceremony in July 2017.

Shazwani Babjee of the Home Team Training and Learning Office at the Home Team Academy caught up with Dr. Naresh to discuss his latest project, the Mobile Classroom or MobiC.

Why is technology important for Home Team Transformation? In particular, how can technology be applied to training and learning?

Technology has been, and will continue to be one of the key enablers of our Home Team Transformation.

We have already seen how developments in the field of science and technology have radically changed the way Home Team op-

erations are conducted on multiple fronts. ICA, for one, uses video analytics for persons-of-interest identification and the Automated Biometric and Behavioural Screening Suite for the tracking of suspicious persons at land checkpoints. CNB's Automated Image Processing System uses robotics to automate administrative tasks, saving manpower and time. (See box for details.)

With the appropriate attention given to science and technology, the Home Team can rise above its challenges in the fields of law enforcement, terrorism, border security and emergency vulnerabilities, and disrupt and diffuse the ill consequences these challenges pose to society. Technology has the potential to raise the bar of human judgement for the better.



Figure 1. Dr. Naresh Kumar (right) receiving the Innovation & Development (Individual) Award from Minister for Home Affairs K Shanmugam. (PHOTO: AIZIL A.RAHIM)

Automatic Biometric and Behavioural Screening Suite (ICA)

The Automatic Biometric and Behavioural Screening Suite (ABBSS) uses real-time facial recognition capabilities to quickly sieve out suspicious persons against databases and track them. It is also able to recognise vehicle numbers, spot unattended baggage, and track objects based on colour, shape and size. ABBSS has been effective in enhancing security at the Woodlands Checkpoint and for several large-scale events since 2012.

Automated Image Processing System (CNB)

Rolled out in 2016, the Automated Image Processing System has sped up CNB's manual process of handling photographs taken on scene. With the aid of a robotic arm, the system automatically backs up the contents of SD cards into DVDs and stores them. The system also automatically prints, sorts, and binds case photograph albums for investigative and prosecutorial purposes. The time savings achieved mean that officers can now spend more time on higher value work.

“ With the appropriate attention given to science and technology, the Home Team can rise above its challenges in the fields of law enforcement, terrorism, border security and emergency vulnerabilities, and through this, disrupt and diffuse the ill consequences these challenges pose to society. Technology has the potential to raise the bar of human judgement for the better. ”

– Dr. Naresh Kumar,
Director OCSTO & HF

Similarly, technology, when designed for training and learning, can be an effective tool in enhancing the Home Team’s operational effectiveness and readiness.

For instance, we have seen how technology based e-training programmes, such as the Home Team Learning Management System (HTLMS), have impacted our officers. They can now learn at their own pace at the click of a mouse. (See below.)

In fact, there are also other ways in which technology can be applied to training and learning such as VR and Augmented Reality (AR). Project MobiC is one such initiative that adopts both these technologies.

There has been discussion within the Home Team about the need to tighten the “Ops-Training Loop”. Where does MobiC fit into this and why is it important to the larger Home Team Training Transformation?

First, let me start by saying that our officers on the ground think that there is little operational downtime available for training. Their views are reinforced by their personal experiences, where each course is at least half a day long, excluding travelling time! Over time, they have naturally assumed that if they do not have a clear window of opportunity to train, they then do not have the time for learning. We wanted to correct this perception. Training is absolutely vital to the continued effectiveness of the Home Team in dealing with evolving threats and challenges. On-the-job training, though necessary, is in-

Home Team Learning Management System (HTLMS)

- The HTLMS is a centralised learning platform for training and learning activities across all Home Team Departments. It is the first Home Team unified learning platform.
- Every Home Team officer has a HTLMS account.
- Officers are able to access many learning resources online 24/7.
- Enables learning ‘anytime, anywhere’.
- Allows each Home Team Department to disseminate training content to all officers.
- Enables cross-department learning and sharing of content.

creasingly no longer sufficient. Our frontline officers need to exercise the right judgement and reflexes when confronted with a real life situation, be it a knife wielding terrorist or at a crime scene. We need to give them the tools to build their confidence and hone their judgement on a daily or weekly basis.

Second, part of the Home Team Training Transformation involves inspiring a culture of proactive learners. There are many ways to achieve this, one of which is to enhance conventional modes of training and learning with technology. For example, technology in the form of VR simulations can make the training and learning process more appealing, especially to our younger officers. My opinion is that if we can leverage VR technologies to first get our officers interested and involved in up-skilling, then we are on our way to building a culture of proactive learners.

With these two points in mind, I believe we have taken a step in the right direction with the development of MobiC.

How did the concept of MobiC come about and what does it mean to you? What are some of the considerations behind the conceptualisation of MobiC?

The idea of mobile training was mooted by then 2nd Permanent Secretary (Home Affairs), Mr Loh Ngai Seng, during his visit to the Home Team Human Performance Centre in October 2016. During the visit, 2PS said that VR and AR technologies had massive potential, and should be further leveraged to meet the next generation training needs of the Home Team.

Our concept for MobiC was inspired by the series ‘Transformers’. We thought that the concept of a mobile classroom on wheels that could transform into a VR/AR training space was ideal for bringing learning content to the frontline. This content could then be easily updated and conducted in bite-sized modules, in between duties or rotations. We thought this was a good concept, as officers will no longer need extended periods

Mobile Classrooms: What You Need to Know

- MobiC is a customised vehicle platform that leverages VR technology to bring realistic scenarios to the frontline. It can be driven and parked at the various Neighbourhood Police Centres, offering dedicated training space and equipment.
- MobiC was designed with ergonomic and human factor design principles in mind, to ensure a safe and realistic training environment.
- MobiC consists of training in a customised vehicle platform and a ‘classroom’. Up to four officers can train on the platform, and another 12 in the classroom.
- MobiC was developed by OCSTO in collaboration with SPF and HTA.

of downtime for training. Furthermore, VR/AR technologies not only serve to inject realism into the training, it also makes the whole training experience engaging and interactive for our officers, which is definitely a plus for them.

Apart from the use of advanced VR/AR technologies, MobiC was designed with human factors engineering principles in mind, to enhance performance in virtual environments. This allows our officers to maximise their capabilities, and at the same time, ensures that the space limitation of the mobile platform would not be an issue for the officers to train in for extended periods of time.

Overall, we wanted MobiC to deliver realistic and highly customisable VR scenarios to train our police officers deployed at the Neighbourhood Police Centres. This will allow them to refresh and practise their skills when responding to dynamic operational situations in a safe, realistic and efficient learning environment.

What were some of the problems encountered by the team, and how were they resolved?

One area that we found to be a challenge was the space restriction. Specifically, it was an engineering challenge, as we had to create an expandable mobile platform to house training and learning technologies that can meet LTA's road vehicle requirements. We had to consider the load and capacity requirements of about 3,000 kg and 28m² in such a way that it was comfortable and conducive for training a team of officers. At that time, there wasn't a reference in the market for us to start with. It was through bringing together our expertise in technology, platform design and our understanding of human limitations, that we were able to design a solution that met the

“ *Enhancing frontline training is a step towards the right direction. As the MobiC training sessions would be conducted before patrol shifts, the lessons learnt would be fresh in officers' minds when they perform their duties.* **”**

**– Sergeant Anderitte Lim,
Bedok North GRF officer**

spatial, physical and cognitive requirements of the users.

How will MobiC impact frontline training and the Home Team as a whole?

The Home Team is constantly recruiting newer generations of officers who are highly qualified, technology-savvy, and eager to perform well in the roles and responsibilities assigned to them. Hence, officers must be given access to the most effective training programmes when they are deployed to critical frontline duties. To achieve this, our officers must be equipped with on-the-go skillsets that are tailored to their specific operational needs.

Secondly, 'pen and paper' methods of teaching and classroom-based training can now be augmented by technology to ensure our officers are always equipped with up-to-date skills. These are exactly what MobiC aims to deliver.

What's next for MobiC?

We are currently undergoing the proof-of-concept (POC) for MobiC. Our focus for the POC is on determining the effectiveness of using VR technologies in SPF's frontline training, and also to enhance several of MobiC's features. If this POC is successful, more

MobiC vehicles may be commissioned and rotated amongst the Neighbourhood Police Centres. We will also begin exploring how MobiC can be adapted for use in other Home Team Departments.

The plan for the longer term would be to develop new VR content and training materials, and expand on the human factors component of the MobiC. These add-on modules will track and better evaluate an officer's performance. For example, eye tracking technology can be used to assess an officer's focus in a crime scene investigation or shoot-out scenario, and an officer's state of emotion could be tracked by monitoring his anxiety and stress levels. From these statistics, better feedback could be provided to officers, to achieve higher levels of performance and efficiency.

Do you see technology being used even more for training in the future? Where do you see this heading?

The future operating landscape will afford us

less operational downtime with increasing workload demands and a shrinking population. Naturally, there will be a growing reliance on technology to help alleviate some of these demands.

I envision that new and emerging technologies will become deeply entrenched in many areas of the Home Team, especially in the training and learning ecosystem. Trainees will have access to training and learning content personalised to their needs, which will allow them to take charge of their own learning journey. Trainers will be empowered with the tools needed to deliver content in the most effective and efficient manner, as well as to assess individual progress and needs of trainees. Various systems will be put in place for the quick delivery of training to the front-line and to identify training areas that require more attention.

I look forward to a transformed Home Team in 2025, and am excited to see how technology will shape training and learning over the next two decades.

Benefits of Training with MobiC

- MobiC reduces training resource requirements. The normal mode of training needs physical training facilities, trainers, equipment and role players. Using VR technologies require much fewer resources.
- The mobile platform allows increased training frequency – training can be done at the same time for multiple units in a virtual environment using VR equipment.
- Highly configurable, scalable and replicable – unlike a physical training facility setting that is limited by space and not easily reconfigured, MobiC allows for many training scenarios to be created. These scenarios can involve single or multiple trainees and can be consistently re-created.
- MobiC has a small footprint. The space required to set-up a VR workstation can be as small as 3m by 3m.

“ Training is the only way to prepare officers to perform their jobs well.

To our leaders – the senior management in Home Team Departments, commanding officers, and team leaders on the ground – my advice is, lend your support to your trainers, both full time and adjunct. Work closely with your Chief Learning Officers to effect change within your own organisation, and communicate these changes frequently to officers, so that they know what they are about to experience, and are ready for the future.

To our trainers, you are the key to a successful training transformation. As trainers, you must exemplify the ideals of lifelong learning. Take time to participate at the Home Team Trainers’ Day held every May and November to learn more about what others are doing within and beyond the Home Team.

To our officers, you have a key role to play in the training transformation. Be proactive, provide constructive feedback on your training experience, and participate actively to make the most out of your training time.

A highly and better trained Home Team will result in a safer and more secure Singapore.”

– Loh Ngai Seng
2PS (Home Affairs)
January 2016 to August 2017



About the Author

Shazwani Babjee is a senior executive with the Home Team Training and Learning Office at the Home Team Academy. Her work involves strategy formulation and planning for the Home Team’s training and learning ecosystem. She is also an editor for the Trainers’ Quarterly, a news bulletin to keep trainers updated on the latest training technologies, adult pedagogies, curriculum and all matters related to training and development.

Growing Thought Leadership and Capacity in Safety and Security

By Jason Jevanathan
Institute of Safety and Security Studies

To grow the Home Team's future readiness to deal with emerging threats and security trends, the Institute of Safety and Security Studies (ISSS) was established on 1 January 2017. Located at the Home Team Academy, the vision of ISSS is to establish Singapore as a safety and security (S&S) capacity building and thought leadership hub.



The primary mission of ISSS is to provide specialist professional development and training in the safety and security disciplines to enhance the overall capability of Home Team departments, Homefront agencies and key local stakeholders to ensure a safe and secure Singapore.

A successful and credible ISSS can also serve the Home Team's external interests. ISSS gives the Home Team a platform to build and enhance its networks of foreign counterparts and S&S practitioners whom the Home Team can call upon in times of need. By offering capacity building programmes, such as the ISSS-ASEAN Cyber Investigators Course, to foreign counterparts, ISSS can also cultivate and nurture a network of ASEAN experts in S&S practices and standards and help keep our region safe.

ISSS consists of 3 main centres: the Centre for Protective Security Studies (CPSS), the Centre for Cyber Security Studies (CCSS), and the newly established Advocacy Office against Drugs and Crimes (AODC).



CPSS was established on 1 January 2012 to raise protective security standards in Singapore. To achieve this, CPSS provides protective security training and advisories to stakeholders and manages key security programmes such as Red-Teaming and TOPSIS (Threat Oriented Passenger Screening Information System).

Besides training Home Team officers, CPSS also extends its training modules like Protective Security Principles, TVRA (Threat, Vulnerability & Risk Assessment) and TOPSIS Tell-Tale Indicators (TTIs) to Homefront agencies and key external stakeholders.



CCSS was established on 1 July 2014 to serve as a centralised body to facilitate capability and capacity development of Home Team Departments and key stakeholders in the areas of cyber security, cybercrime and investigation.

CCSS achieves this by delivering skills-based training at its Cyber Security Lab to level-up the competency of Home Team staff. The centre also collaborates with research institutes, institutes of higher learning and industry stakeholders on cyber security research and the development of cyber security and cyber-investigation programmes.

AODC was established on 1 January 2017 to further the Singapore government's advocacy efforts against illicit drugs and transnational organised crime and to promote counter-terrorism initiatives, both domestically and internationally, to strengthen alliances already present, as well as to create new alliances.



In collaboration with the Home Team, other government departments and non-governmental agencies, the AODC aims to advance Singapore's position in the international arena as a responsible global citizen and thought leader while concurrently safeguarding national policy and securing Singapore's interests. Domestically, the AODC's advocacy efforts currently focus on gaining support for Singapore's robust policies on the control of illicit drugs through outreach programmes to reach out to key local constituencies.

ISSS is still a very young institute. There is still much work to be done. While its roles and functions will likely evolve over the coming years in line with shifts in the S&S landscape, ISSS will continue to strive for excellence in its mission to enhance capabilities in the S&S disciplines.



About the Author

Mr Jason Jevanathan graduated in 2009 with a Masters in Management of Security Studies from the Edith Cowan University, Western Australia. As part of his final research paper, he successfully articulated a framework for resilience for Singapore through the lens of two national episodes: the SARs epidemic in 2003 and the Mas Selamat escape in 2008. Jason is not only a trainer within the Home Team community, but also an adjunct lecturer with the University of Liverpool in the UK and Temasek Polytechnic in Singapore. He is also regularly invited to speak at the S Rajaratnam

School of International Studies and other local institutions. His paper on "The 2008 attack on Kabul Serena Hotel: Lessons from a Captured Suicide Bomber" (co-written with Susan Sim) was published by the NATO Centre of Excellence Defence Against Terrorism in May 2011 and regularly given out to course participants. In 2016, he attained a Diploma in Adult & Continuing Education (DACE).

Jason is currently the Senior Assistant Director of Partnership Development at the Institute of Safety and Security Studies (ISSS). He is responsible for supporting ISSS as a Centre of Excellence for Safety and Security by developing valued partnerships with all stakeholders concerned with the safety and security of Singapore.

Building a Vibrant Eco-system for the Home Team to Deal with Cybersecurity & Cybercrime Threats

By Michael Ong
 Centre for Cyber Security Studies
 Institute of Safety & Security Studies

The Home Team must be resilient against cyber-risks. We must secure our systems on the Internet, particularly those systems deemed to be critical infrastructure, so that we can confidently use them in our daily operations and service provision to the public. At the same time, the Home Team must develop capabilities and capacities to effectively investigate and deal with cybercrimes, crimes that are transacted via cyberspace and serious cyber breaches that involve security or criminal investigations. To deal with both threats, the Centre for Cyber Security Studies (CCSS) is developing a cybersecurity eco-system for the Home Team that will also facilitate collaboration between Home Team departments, CCSS and other partners.

Cyber-Risks and Public Service Efforts

Singapore has experienced rapid growth in e-commerce over the last few years. With the growth in e-commerce, Singapore has also experienced a rise in cyber-attacks targeted at businesses and private sector organisations. Even retail malls like Tiong Bahru Plaza and

White Sands were not spared and were affected by the “WannaCry” ransomware attack in May 2017. Many countries, organisations and individuals were also impacted by the NotPetya ransomware that wreaked much havoc in June 2017.

Singapore takes cyber-risks very seriously because our inability to deal with cyber-attacks can result in a loss of reputation for Singapore. The public service started to take active steps in May 2016 to separate internet surfing from government networks. At that time, cyber security attacks on public and private sector organisations were already on the rise. The Singapore Government had been the target of various Advanced Persistent Threats (APTs), which sought to breach our ICT systems and compromise data. By May 2017, all public servants were no longer allowed to surf the Internet using computers linked to government networks. At the same time, measures were put in place to ensure the service level of public e-services and email communications between public officers and citizens were neither disrupted nor reduced.

The Need for an Ecosystem

Both the National Cybercrime Action Plan (MHA 2016) and the National Cybersecurity Strategy (MCI 2017) recognise the need for an extensive cybersecurity and anti-cybercrime eco-system. Partnership and eco-system building stands as a distinct and important pillar of both plans, necessitated by the complexity and scale of the challenges posed by cyber security and cybercrime threats. Adversaries are not just lone hackers but range from organized cyber-criminal groups, to state sponsored cyber-criminals (Venable 2015) and espionage groups (Zetter 2015). These adversary groups have their own eco-systems, such as forums for trading of tools and technologies (Maor 2015, KrebsOnSecurity 2015). With the advent of leaked state-developed cyber tools, such as those revealed by Wikileaks, threat actors and criminals can leverage weaponised cyber tools for their own nefarious purposes. The Wanna-Cry and Petya ransomware attacks that affected the UK National Health Service (BBC 2017) and forced international shipping Company Maersk to use paper records (Chambers 2017) were enabled by the EternalBlue Windows exploit that was alleged to have originated from a state security agency. These are examples of the chaos that can result when such state-developed tools are released and used by other actors.

Furthermore, technology and innovation in cyber applications progress at a rapid pace across multiple sectors and disciplines, with implications for investigations into traditional crime as well. How should investigators deal with a kidnap-for-ransom case if the ransom is demanded in crypto-currencies that protect the identities of the perpetrators? How should a computer be inspected if it is an Internet-Of-Things device such as a refrigerator or

a smart television that is used in the commission of a cyber-enabled crime? How do we get ourselves ready to deal with crime and security in a Smart Nation? The scope of the cybersecurity and cybercrime challenges requires us to harness talent and expert knowledge beyond the Home Team to deal effectively with these threats.

Examples of Ecosystems

We are not alone in identifying the need for an eco-system. The US Department of Homeland Security developed a strategic blueprint to establish an eco-system of collaborators from industry, academia, local and overseas governmental entities to collectively develop capabilities to secure the Cyber Future of the United States (Department of Homeland Security, 2011). According to academics Bauer and van Eeten, such government-led collective framework is intended to reap cybersecurity enhancing benefits in the fight against cybercrime and cybersecurity threats (Bauer and van Eeten, 2009).

In Israel, the CyberSpark initiative was launched in January 2014 (SecurityWeek News, 2014) to bring experts and partners from industry, academia and public sector agencies such as the Israeli Defence Force within close physical proximity to foster closer collaboration and seeding of ideas and innovation in cybersecurity. Major enterprises such as Lockheed Martin and IBM joined Deutsche Telekom, EMC and RSA by committing to invest in Beer-Sheva's Advanced Technologies Park. While the CyberSpark initiative had several different economic and geo-political objectives, one of its main goals was to enable Israel to continue to excel in cybersecurity innovation.

Building an Ecosystem for the Home Team

It is therefore imperative that the Home Team builds a vibrant eco-system comprising collaborators from the industry, academia as well as strategic partners locally and around the region in order to combat these threats too, particularly to deal with cybercrime.

The mandate of the CCSS is to support Ministry HQ and Home Team departments (HTDs) in competency and capability development in cybersecurity and cybercrime investigation through applied research and development and training. To fulfil its mission, CCSS adopts a three pronged strategy of CONNECT, CREATE and EDUCATE. (See Figure 1.)

Each of these strategy planks have specific goals, viz.:

- **CONNECT** – To establish networks of people and organisations from academia and industry with expertise in cybersecurity and cybercrime investigation. The intent is to create a network conduit for MHA to exchange information and learn from local and global cyber experts and leverage their capabilities and expertise to enhance HTDs’ capabilities in cybercrime and investigation.
- **CREATE** – To establish technology platforms for collaboration and to drive the development of cybersecurity and cybercrime investigation tools for MHA. Such platforms will provide the means for MHA to conduct technology trials and experimentations with the communities from academia and industry. The platforms will also facilitate the transition of R&D and prototype tools to operational applications by HTDs.
- **EDUCATE** – To drive the competency development of Home Team officers through

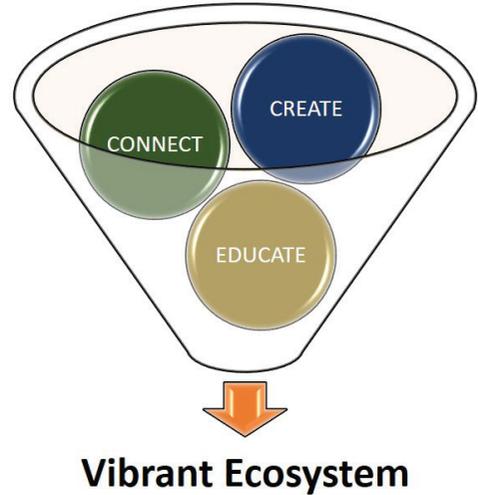


Figure 1. CCSS's three pronged strategy of CONNECT, CREATE & EDUCATE

training and learning. Through a mixture of in-house and external courses and seminars, participants will be equipped with the knowledge and skills to deal with current and future threats. As part of the mission of the Institute of Security Studies (ISSS), it will also support specific areas of competency development of regional partners of Home Team agencies in areas such as cyber forensic investigations, as part of larger engagement strategies.

Overview of Initiatives

Some key initiatives undertaken by CCSS are:

• Special Interest Group in Cybercrime & Investigation

CCSS established the Special Interest Group (SIG) in Cybercrime and Investigation with the Singapore Cyber Security Consortium (SGCSC) in June 2017. The objective of forming the SIG is to gather and direct the community of cybersecurity experts towards innovating and developing cybercrime fighting capabilities for MHA. This SIG will also provide an avenue for establishing network links to the cybersecurity expert community to acquire relevant knowledge and capabilities in

cybercrime and investigation for HTDs. The partners include the National Research Foundation (NRF), with involvement from local universities (National University of Singapore, Nanyang Technological University, and Singapore Institute of Technology) as well as participation from industry.

• ASEAN Cyber Investigator Course

The primary objective of this programme is to CONNECT with law enforcement officers from ASEAN member states through training and sharing of cybercrime cases and expertise. The course equips trainees with investigation and digital forensics competencies to conduct cybercrime investigations, through hands-on exercises and case studies. The Level 1 course runs were successfully conducted in November 2016 and August 2017. Participants from Brunei, Indonesia, Laos, Malaysia, Myanmar, Thailand, Philippines and Vietnam attended and were joined by officers from SPF, CNB and ISD. The first run of the Level 2 course was held in November 2017.

• Temasek Advanced Learning, Nurturing And Testing Laboratory (TALENT)

The TALENT Lab is a joint collaboration be-



Figure 2. CCSS at the Special Interest Group in Cybercrime and Investigation.

tween MHA and Temasek Polytechnic. Its purpose is to foster deeper cooperation between the Home Team and Institutes of Higher Learning (IHLs) in the areas of cyber-forensics and cyber-investigations as well as to facilitate the sharing of knowledge and ideas among staff and students from different IHLs. The Lab will also train students aspiring to work on cybercrime and cyber investigation problems, including cybercrime detection, analysis, investigation and evidence preservation. It will serve as a platform for the conduct of applied R&D projects on the latest cyber investigation technologies which are of interest



Figure 3. President Tony Tan with students and staff of Temasek Polytechnic, hosted by former 2PS Loh Ngai Seng and TP Principal/CEO Peter Lam at the TALENT Lab.

Job Functions Identified

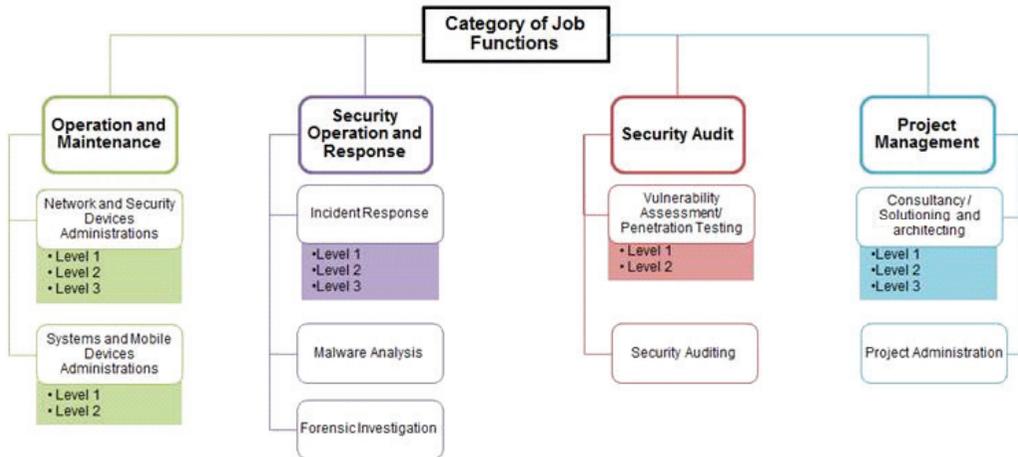


Fig 4. Cyber Competency Framework.

to the Home Team.

• Cybersecurity Competency Framework

Training is a core function of CCSS. Commercial cybersecurity courses are already available for anyone keen on picking up cybersecurity skills. It is therefore critical that CCSS' courses are unique and optimised for the Home Team. CCSS has developed a customised Cybersecurity Competency Framework, focusing first on Home Team officers involved in the management, development, operation and main-

tenance of critical Home Team Information Communication Technology (ICT) systems, to facilitate the training and equipping of such officers with requisite ICT security competencies. With the competency framework, officers have greater clarity on the competencies required for their role and can play their part towards securing their department's ICT systems.

Since the Cybersecurity Competency Framework was formalised in November 2016, three new courses have been made available for Home Team officers while another four modules will be rolled out in 2018. More than a hundred officers from across the Home Team have been trained. Concurrently, the next version of the framework is being refreshed and expanded to include operational and specialist roles in cybersecurity and cybercrime investigations.

“... the course is very important to all cybercrime investigators of ASEAN. Also of equal importance is the link developed by investigators towards oneness of purpose to combat cybercrime across borders.”

– Rojun Hosillos,
Cybercrime Division,
National Bureau of Investigation,
Philippines

Conclusion

Cyber threats will continue to evolve and pose a daunting challenge to the Home Team. Op-

erational units within the Home Team will therefore need to develop the competency of its officers and grow their technical capability to stay ahead of these challenges. CCSS seeks to address these challenges and needs through its three prong strategy of CONNECT, CREATE and EDUCATE. Moving forward, CCSS will continue to work alongside operational

counterparts to boost collaborative research and training in preparation for Home Team Transformation 2025.



About the Author

Mr. Michael Ong joined the Ministry of Home Affairs in 1998 and has served in various technology related areas. He was appointed Executive Director, Centre for Cyber Security Studies in September 2016. As ED CCSS, he is focused on developing the centre's competencies and offerings to the Home Team in the areas of cyber security threats, cybercrime and cyber investigations. He holds Masters degrees from the Nanyang Technological University (NTU) and Cambridge University.

References

- BBC (2017, May 2013). Massive ransomware infection hits computers in 99 countries. *BBC News*. Retrieved from <http://www.bbc.com/news/technology-39901382>
- Bauer, J. M. and van Eeten M. J. G. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications policy*, Vol. 33, Issue 10-11, p. 706-719, Nov-Dec 2009.
- Department of Homeland Security (2011). *Blueprint for a Secure Cyber Future*. Retrieved from <https://www.dhs.gov/blueprint-secure-cyber-future>.
- Chambers, S. (2017). *Back to the future for Maersk in the wake of Petya attack*. Retrieved from <http://splash247.com/back-future-maersk-wake-petya-attack/>
- KrebsOnSecurity. (2015). *The Darkode Cybercrime Forum, Up Close*. Retrieved from <http://krebsonsecurity.com/2015/07/the-darkode-cybercrime-forum-up-close/>
- Maor, E. (2015). *Cybercrime Ecosystem: Everything is for Sale*. Retrieved from <https://securityintelligence.com/cyber-crime-ecosystem-everything-is-for-sale/>
- Venable, D. (2015). *State-sponsored Cybercrime: A growing business threat*. Retrieved from <http://www.darkreading.com/vulnerabilities---threats/state-sponsored-cybercrime-a-growing-business-threat/a/d-id/1320555>
- SecurityWeek News (2014). *IBM and Lockheed Martin Invest in Israeli Cyber Complex*. Retrieved from <http://www.securityweek.com/bim-and-lockheed-martin-invest-israeli-cyber-complex>.
- Tabansky, L. & Ben Israel, I. (2015). Cybersecurity in nation state digital attacks. *Wired* magazine, September 2015, p. 33. Retrieved from <https://wired.com/2015/09/cyberwar-global-guide-nation-state-digital-attacks/Israel>.
- Griffin, A. (2017). Wikileaks CIA files: The 6 biggest spying secrets revealed by the release of Vault7. *The Independent*. Retrieved from <http://www.independent.co.uk/life-style/gad>

The Growing Need for Advocacy against Illicit Drugs

By Dr. Rozlan Giri, Sivaraman Letchumanan and Nur Asyikin Hamzah
Advocacy Office against Drugs and Crime
Institute of Safety & Security Studies

“ *Between now and 2019, we need to come to a consensus on how we can move forward as one global community, to tackle drugs. Every country should have the right to choose the approach that works best for them.*

For us, the choice is clear. We want a drug-free Singapore, not a drug-tolerant Singapore. We want to be part of a drug-free ASEAN. ”

– K Shanmugam,
Minister for Home Affairs and Minister for Law
Singapore Statement at the United Nations General Assembly
Special Session on the World Drug Problem (UNGASS)
21 April 2016

Singapore’s robust anti-drug approach is well-known and there are many countries that subscribe to the same drug-free approach.¹ However the global discourse on drugs is becoming more fractious, with the morphing harm reduction movement – beyond health measures – gaining traction. This article discusses the growing challenges to Singapore’s position on

drugs and the importance of developing a new global consensus or at least ensuring that we have sufficient policy space to implement drug policies that work for us and ensures Singapore’s safety and security. An accompanying story describes the work being carried out by the Advocacy Office against Drugs and Crime (AODC) set up by the Ministry of Home Af-

¹ The drug-free approach adopted by Singapore, which involves preventive drug education, punitive sanctions, enforcement efforts, and compulsory drug treatment and rehabilitation initiatives is widely ascribed by other countries, albeit in varying iterations. Some examples of countries that adopt a drug-free approach include China, Malaysia, Hungary, Sweden, and Iceland, where in spite of services such as needle-exchange programmes and substitution therapy, the overarching principle guiding their drug policy remains contributive to a drug-free goal. The 2016 UNGASS Outcome Document also serves to attest the mutual consensus by member states, to “promote a society free of drug abuse”.

fairs to help maintain international and domestic support for Singapore's tough stance on the production, supply and consumption of illicit drugs. Singapore's drug-free approach needs to be articulated at the international and regional levels so that every country can retain its sovereign right to deal with the drug problem based upon its domestic circumstances and conditions.

Singapore's position is science and evidence-based: we take the position that illicit drugs are detrimental to individuals who misuse them. The negative effects extend to abusers' families and communities. Many medical studies have shown that drug abusers experience altered brain chemistry, suffer health complications, and risk tragic death (National Institute on Drug Abuse, 2014; Substance Abuse and Mental Health Services Administration, 2004; Crisp and Barber, 1997; Hoffman, Nadelmann, O'Hare, 1993; Black, 2016). Drug addicts invariably wound their families and communities economically, emotionally and socially. The families, his or her community and the community at large are also adversely impacted as it is usually difficult for addicts to overcome their addiction, often trapping their families in a cycle of poverty and sometimes perpetuating the addiction through generations (Office of National Drug Control Policy, 2000; Jason, Davis, Ferrari, Bishop, 2001; Sterling, Gotheil, Glassman, Weinstein, Sero, Lundy, 1997; Palamer, Kiang and Halkitis, 2012).

The cost of drug addiction to the individual, his family and society is far from trivial.² Furthermore, the nexus between the illicit drugs trade on the domestic and international fronts, and organised crime and terrorism across borders has been attested to globally. There is therefore wide recognition that to achieve success in the fight against the drug menace, drug control must be pursued as a transnational endeavour. A global consensus must underpin this pursuit (United Nations, 2015). Indeed, the fight against drug trafficking and abuse constitute, in modern times, one of the oldest forms of co-operation between countries. As chronicled by Tammi (2014), the first multi-national drug control initiative was the Shanghai Opium Commission of 1909, which saw 13 countries including Great Britain, Japan, China, and Russia convening to address the illegal production, trade and use of opium in China. The conference was a catalyst for countries to pass domestic legislation addressing drug problems within their borders, and united countries in an international co-operative effort to address the problem of the opium trade. The work of the Commission led to the convening of The Hague Opium Conferences (1912-1914) and the adoption of the first international drug control treaty, the 1912 International Opium Convention, along with other succeeding treaties that effectively restricted opium production and trade (American Society of International Law, 1911; Tammi, 2014; Bewley-Taylor, 2012).

² Drugs cost its users, his or her family and community directly through poorer physical and mental health prospects, and indirectly through income loss, and reduced productivity and life quality (Rivera, Casal, Currais, 2017; Quello, Brady and Sonne, 2005). Financial and social costs of drug users' families, have also been shown to occur in the form of income loss due to absences from being imprisoned and the users' inability to work (Rivera, Casal, Currais, 2017). Attributed either by neglect or abuse, or both, children of drug-using parents have been found to present affect dysregulation, and have higher risk of depression, anxiety disorders and substance abuse issues (Whitesell, Bachand, Peel and Brown, 2013; Lander, Howsare, and Byrne, 2013). A cost-of-illness study in Spain found the social cost of drug consumption in 2012 to be between 1,436 and 1,651 million euros - 0.14% of Spain's GDP for that year. Such results emphasize the burden that illegal drug consumption presents for the country (Rivera, Casal, Currais, 2017).

“We are located in a difficult environment. We are near several major drug production centres. We believe that drugs will destroy our society. With 200 million people travelling through our borders every year, and given Singaporeans’ purchasing power, a soft approach will mean our country will be washed over with drugs. This is why we have adopted a comprehensive, balanced, sustained and tough approach to tackling both drug supply and demand. The results speak for themselves. We are relatively drug-free, and the drug situation is under control. There are no drug havens, no no-go zones, no drug production centres, no needle exchange programmes. Our stance on drugs has allowed us to build a safe and secure Singapore for our people. ...

“Demand reduction doesn’t have to mean no compassion or consideration for the drug abuser. It doesn’t have to mean that we lock up the abuser, throw away the keys, and condemn him to a life of criminality. It is possible to be tough on traffickers, be tough on prevention, be tough on drug abusers. And, at the same time, help abusers psychologically, medically, economically, without having to feed them with drugs. It is possible to help many of them kick their habit and reintegrate into society. ...

“This is difficult and resource-intensive. But because every life is important, we do that. Legalizing and giving abusers drugs is the easier option. But not the better one. Believing in the individual, believing that he can be drug-free and can kick the drug habit, believing in human potential. That is the more difficult but better option.”

– K Shanmugam
Statement at UNGASS 2016

A Fracturing Global Consensus

Yet, despite the rich evidence pointing to the staggering costs of drug abuse that individuals, their families and societies bear, there is a growing effort across the globe, often articulated euphemistically using the vehicles of human rights, health care, scientific research and/or the efficacy of drug control policy, to liberalize the drug trade³ and drug use (Stevens, 2011; Bonello, 2015; Mosher and Yanagisako, 1991). These efforts have morphed into a social movement that aims to disrupt the existing global accord on drug prohibition. The sudden proliferation of drug liberalisation advocates on the international scene has been described as nothing less than “startling” (Tammi, 2014). The movement is flush with money deployed for the setting up of non-governmental organisations (NGOs), and for the expansion of research and advocacy favouring a more liberal drug policy (Bridge, Hunter and Lazarus, 2012; Narayanan, Vicknasingam, and Md. Haris Robson, 2011; Rahman and Crofts, 2013). The movement has also cultivated strong enough support from among policy makers and special interest groups to influence domestic drug control policies in a number of countries. These more liberal policies come in various forms, including the decriminalisation of drug use,⁴ the push for the management of drug abuse to be moved away from a country’s criminal justice system and onto its health system, and the adoption of a harm-reduction

³ For example, see <https://arcviewgroup.com>.

⁴ The European Monitoring Centre for Drugs and Drug Addiction (EMCDDA, 2001) defines ‘drug decriminalisation’ as the removal of a conduct or activity from the sphere of criminal law and may include either the imposition of sanctions of a different kind (administrative) or the abolition of all sanctions; other (noncriminal) laws then regulate the conduct or activity that has been decriminalised. ‘Drug legalisation/ de legislation’ requires ending government-enforced prohibition on the distribution or sale and personal use of illicit substances. Drug legalisation may come in various forms of regulated legalisation. These include full legalisation where all drugs are legally available albeit under a system of government control, which might include mandated labels on dosage and medical warnings and restrictions on advertising (Proceedings of the Special Committee on Illegal Drugs, 2001).

paradigm that seeks to minimise the harm suffered by a drug abuser instead of preventing the harm and helping him abstain from illicit drug use (Rahman and Crofts, 2013; Nutt, 2012). These policies are a sea change from the longstanding drug-prohibition approach that criminalises drug production, trafficking and consumption, considers illicit drug use as morally wrong, and argues that society should not condone drug use behaviour due to its detrimental effects (Jakubiec, Kilcer, and Sager, 2009; Bewley-Taylor, 2012).⁵

While it is the sovereign right of countries to devise and implement their own drug control policies, governments would find it difficult to stave off the influence of the liberalising drug movement on their domestic drug policies unless they shape the discourse upstream. After all, current drug control policies, laws and regulations stand on the empowering edifice of a global consensus against the drug trade and drug abuse, first exemplified by the 1961 UN Single Convention on Narcotic Drugs, and further boosted by the 1971 UN Convention on Psychotropic Substances and the 1988 UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (UN, 1961; UN, 1971; UN, 1988; Lande, 1962; Bewley-Taylor, 2012).

Singapore, in particular, has been successful in its fight against drugs. We have one of the lowest prevalence rates of drug abuse in the world (Central Narcotics Bureau, 2016; UN, 2006).⁶ Our safe and drug-free streets are due to our comprehensive national drug policy approach, comprising upstream preventive education efforts, tough enforcement and legislation as deterrence, and downstream correctional rehabilitation efforts for drug offenders, including aftercare support to help ease an abuser's reintegration into his community and society. As circumstances change with new research and scientific evidence, and drawing on lessons learnt, our authorities continually review, refine and improve the drug control policy and legislation. But Singapore has to be careful to ensure that it does not change and weaken the very fundamentals that represent the key success factors in our country's fight against the scourge of drugs. There is a risk that a new international climate marked by a fracturing global consensus on how the drug menace ought to be fought will undermine these fundamentals, and hamstring efforts to battle the drugs menace.

Attempts to influence and fundamentally change the global climate towards the drug problem were visible at the UN General As-

⁵ The 1961 Single Convention on Narcotics Drugs was an attempt to consolidate international treaty organisations dealing with the control of narcotics drugs while making provisions for the control of production of raw materials for narcotics drugs. The 1971 UN Convention on Psychotropic Substances specifically acknowledged the increasing dangers posed by psychotropic substances in terms of public health and social problems and was aimed at controlling the illicit trafficking of this variety of drugs, in particular. The 1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances constituted an update of the two earlier conventions. It emphasised international cooperation and established legal frameworks that took cognizance of the international dimension of drug trafficking (UN, 1961; UN 1971; UN, 1988).

⁶ The Drug Report Situation published by the Central Narcotics Bureau (CNB) in 2016 reported that the number of drug abusers saw a two per cent decrease from 2015 (CNB, 2016). The UN World Drug Report 2006 reported that Singapore's annual prevalence of abuse (as percentage of the population aged 15-64) was amongst the lowest: 0.0002 for cocaine, 0.004 for opiates, 0.004 for cannabis, 0.005 for amphetamines, and 0.004 for ecstasy (UN, 2006).

sembly Special Session on Drugs (UNGASS) 2016 where worldwide drug policy was intensely contested during debates that were far more robust than previous such sittings. Significantly, one large jurisdiction, Canada, which used to be tough on drugs, is gravitating towards legalising recreational marijuana use (BBC, “Canada Unveils Plans”, 13 April 2017). Indeed, while the eventual outcome of UNGASS 2016 was not inimical to Singapore’s drug policy, it showed up marked paradigmatic differences between countries on their approaches to drug policy.

Importance of International and Domestic Advocacy

The emerging shifts in global narratives regarding drug policies and their potential to undermine Singapore’s drug control regime make it vital that we advocate our position more assertively on the international front. It is imperative that we take an active part in shaping global narratives on drug use. The management of an issue as international as drug control requires a global effort and global consensus. It is crucial therefore, that we continue to advocate that the fight against drug abuse and those who traffic and peddle it must continue, and that there must be policy space for countries that are as tough against drugs as we are, to have the freedom to continue this path to protect our people and our society. While we are open to ideas that work, there is a need for us to ensure that we guard the fundamentals that have led us to successfully contain the drug problem in Singapore over the last five decades. In addition, beyond international advocacy, we have to safeguard our domestic space as well and ensure that Singaporeans support our comprehensive approach to tackling the drug threat.

To be sure, there is substantial domestic support at this time for our policy and approach

against illicit drugs. A public perception survey of some 2,748 youths aged 13 to 30, and 1,212 members of public between the ages of 31 and 60 commissioned by the National Council against Drug Abuse (NCADA, 2016) between 2015 and 2016 found strong support for the country’s drug-free approach. Overall, 81% of those surveyed held negative views towards drugs; over 50% associated drugs with intrinsic harms, such as “affecting one’s body and mind” and “being addictive”. 89% of respondents agreed that Singapore’s drug laws were effective in keeping the streets drug-free; and over 75% supported Singapore’s zero-tolerance approach (NCADA, 2016).

Yet considering how seductive the message is – in its appeal to human rights, and health and policy efficaciousness – one would be remiss and complacent to assume that the message on decriminalisation or even legalisation of drug use will never find significant traction in Singapore. The task of advocacy in these circumstances involves mapping out the key arguments for Singapore’s current national policies against drugs as well as of those holding a diametrically opposed view, examining the premises upon which such arguments are based, evaluating the evidence of how these different approaches have worked, and formulating counter-arguments arguments that are balanced, objective and rational against them.

The essential arguments being purveyed by casual-minded drug advocates instrumentalise the notion of harm reduction. What does it mean and how do we respond to it?

What is Harm Reduction?

The impetus behind the harm reduction approach was the AIDS epidemic (International Harm Reduction Association, 2010; O’Hare, 2007; Stimson, 1995; Stimson, 1990; Advisory Council on the Misuse of Drugs, 1988). The

danger of AIDS spreading from drug users to the general population was assessed as posing a greater threat to the general health of communities and populations compared to the danger of drug-taking itself. It was in these very specific circumstances that harm reduction emerged as a public-health plank of drug policy for AIDS-impacted communities (Bewley-Taylor, 2012). Harm reduction, in this particular regard, was manifested in initiatives such as the needle and syringe programme in places like Amsterdam, Rotterdam and Liverpool (O'Hare, 2007; Erikson, Riley, Cheung, O'Hare, 1997; Stimson, 1995; Santamaria, 2000). It placed priority on reducing the negative consequences of drug use, in this case, the spread of the HIV virus to the general population. Advocates also argued that it was not rational to expect all individuals to make good decisions always, including abstaining and desisting from drugs (Heather, Wodak, Nadelmann and O'Hare, 1993).

Notwithstanding its very particular provenance, proponents of a liberal drugs policy have opportunistically deployed the idea of harm reduction - in its various iterations - to differing contexts of drug use. The notion lacks conceptual clarity owing to this selective use. For instance, some construe it as a strategy while others consider it a goal. Some take it to encompass measures that are aimed at eventually weaning off those addicted to scheduled drugs, while others consider the reform of laws that seek to decriminalise drug possession as an integral part of it (Michels, Stover, and Gerlach, 2007; Bewley-Taylor, 2012; Riley and O'Hare, 2000; Roe, 2005; Reinerman and Levine, 1997).

Harm reduction then gradually became pitted against harm prevention, which refers to "all concerted efforts by civil society, the private sector, and the government to eradicate the harm that drug addiction exacts upon the in-

dividual and collective (family, school, workplace, community and nation) ..." through educating people about the dangers of drug use, policing against drug supply, enforcing tough legislation against trafficking, possession and use, rehabilitating abusers and facilitating their reintegration back into society (Quah, 2017; Tammi and Hurme, 2007).

Regardless of their tactical differences, these harm reduction advocates that have used it beyond its original provenance and intent have one common argument: that drug consumption is a morally neutral and non-deviant behaviour (Harm Reduction Australia, 2015; Tammi 2004). Herein lies its danger: beyond absolving the drug user from responsibility for his or her drug use behaviour, it assumes that the government is obligated to support the addict's drug taking in the name of citizen welfare. Such an approach weighs down a country's health system and imposes a heavy societal cost. Clearly, this approach places untold burden on the financial and human resources of communities and countries in service of an individual's personal choice, when resources could be otherwise channelled to other medical and societal priorities, such as affordable healthcare. There is a major trade-off to be endured, and a huge societal price to be paid. But one hears very little discussion of this trade-off and price.

In this sense, harm reduction has now developed to become a social movement that presents itself as a voice of the unfortunate and excluded (Tammi 2004; Mosher and Yanagisako, 1991). Yet one hears little discussion on the actual aspirations of drug users undergoing rehabilitation (Neale, 1998). Those who uphold the superiority of harm reduction as mere strategy without regard to treat drug users to recovery neglect the perspectives of the drug users undergoing rehabilitation. That drug users prioritize complete abstinence over harm reduc-

tion was demonstrated in a study conducted on 1,007 drug addicts who were starting drug treatment in Scotland. In that study, only 7.1 percent expressed desire for ‘reduced drug use’, 7.4 percent for ‘drug use stabilization’, and less than 1% identifying ‘safer drug use’ as a goal (McKeganey, et al., 2004). The majority of addicts sought complete recovery from the drug dependence as the goal of rehabilitation efforts. Similarly, a separate study in 2007 by the National Treatment Agency (NTA) in England also reported high proportions of 77.5 percent of heroin users, 72.9 percent cocaine abusers and 59.7 percent of those who abuse amphetamines stating their goal from treatment to completely cease drug use (NTA, 2008). Findings from these studies showed that drug users themselves sought abstinence rather than harm reduction as the goal of rehabilitation (McKeganey, 2011; McKeganey et al., 2006).

Decriminalisation and the Case of Portugal

The movement to decriminalise drugs emanates from a paradigm that considers harm reduction as an end in itself (Levine, 2002). Their proponents call for the removal of criminal penalties associated with the use of particular psychoactive substances but retains administrative penalties against users (Tammi, 2004; Levine 2002). It aims to move drug users - deemed as needing medical treatment - from the criminal justice system onto the public health sector and thereby reduce their stigmatisation while facilitating the drug user’s treatment for his or her addiction problems (Rosemarin and Eastwood, 2012; Wodak, 1999; Domoslawski, 2011; Ahern, Stuber, and Galea, 2007).

An example of a country that has adopted this approach to decriminalise drug use is Portugal. In 2001, it decriminalised drugs, includ-

ing cannabis, methamphetamines and heroin (Greenwald, 2009; Domoslawski, 2011). The drastic move was in response to a sustained public health problem that Portugal was grappling with – the high prevalence of HIV, and increased risk of hepatitis B and C pandemics (Vastag, 2009). The fear of incarceration that drove drug addicts underground and the cost of incarcerating people that was assessed to be more expensive than treatment were cited as among the reasons for Portugal embracing decriminalisation (Vastag, 2009). Since then, several major journals such as *The Economist* have held up Portugal as a success (*The Economist*, 2009; *TIME*, 2009; *Scientific American*, 2009). A libertarian think tank, the Cato Institute, lauded Portugal’s drug decriminalisation strategy as a “successful model of harm reduction” with these assertions:

“ ... illegal drug use amongst youths declined, rates of new HIV infections caused by sharing dirty needles dropped, and the number of people seeking treatment for drug addiction more than doubled ... ” (Greenwald 2009)

Yet the glowing report is not well founded. A critical review of the literature on the evaluation of Portugal’s drug decriminalisation efforts reveals a paucity of data to enable a serious before-and-after comparison (Hughes and Stevens, 2012; Hughes and Stevens, 2010). The reality was that Portugal by its approach in 2001 of making drug consumption an administrative offence rather than a criminal offence, was merely formalising an existing policy and practice (Laqueur, 2015). Crucially, data reported by the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) indicated to the contrary that Portugal has suffered an increased number of lifetime drug users across all age groups above 19 years old since drug decriminalisation took effect

(EMCDDA, 2001).⁷

The debate on whether the Portuguese drug decriminalisation program is a success or otherwise confounds, but not because of a disagreement over facts. Rather, it is over which facts matter when it comes to interpreting the results (Hughes and Stevens, 2007; Hughes and Stevens, 2012; Felix and Portugal, 2017). For instance, the Cato Institute report of a decreased rate of lifetime prevalence of cannabis use among Portuguese school students was inferred based on data collected during Portugal's post-drug reform years from 2001 onwards (Greenwald, 2009). Without a before-and-after data analysis, the Cato Institute's data and report is less weighty in measuring the effectiveness of the reform on drug use in the country.

So, Drug Liberalisation?

Another initiative premised on the paradigm that upholds harm reduction as a goal that takes it away from its original intent, is the easing of controls on drugs and allowing for the cultivation, manufacture, processing and retail sale of drugs, even identifying it as a source of fiscal revenue not unlike alcohol and tobacco (Levine, 2002). Proponents of this approach also claim that the transparency in supply, cultivation, production, regulation and retailing of these psychoactive substances enables their safe production and use (Coyne and Hall, 2017; Tammi and Hurme, 2007; Reinerman and Levine, 1997). This in turn, so the argu-

ment goes, will reduce the risk of accidental deaths by overdose, or poisoning from toxic additives. Pro-legalisation groups argue that outlawing drugs undermines the potential effectiveness of health interventions for addicts as drug users are less likely to volunteer to receive treatment and rehabilitation, thereby increasing the rates of deaths by accidental overdose. This argument, however, does not hold in the face of studies that have indicated that most people who successfully complete drug rehabilitation are due to some form of legal obligation (Bai, 2011; Brecht, Anglin and Wang, 2009; Perron and Bright, 2008; Miller and Flaherty, 2000). Very few addicts walk in for treatment on their own. The studies show that most drug users will find it too onerous to even want give up their habit unless it is mandatory for them to do so (Bai, 2011; Brecht, Anglin and Wang, 2009; Perron and Bright, 2008; Miller and Flaherty, 2000).

It is little wonder then that the legal obligation for a drug addict to undergo rehabilitation and treatment has been identified as a strong predictor for positive outcomes in drug rehabilitation (Perron and Bright, 2008; Young and Belenko, 2002). Indeed, studies comparing the effectiveness of mandated and voluntary treatments have shown that the former do as well or better during and after treatment (Perron and Bright, 2008).⁸

An example of a country that makes it compulsory for a drug abuser to seek treatment is Sweden (Reitan, 2016). Sweden adopts a 'zero

⁷ The European Monitoring Centre reported this for Drugs and Drug Addiction (EMCDDA), based on statistics compiled between 2001 and 2007. It indicates that more people took cannabis, cocaine methamphetamines, ecstasy, and LSD after decriminalisation.

⁸ The former is more likely to report abstaining from drugs before their follow-up interview, and demonstrate reduced addiction severity at follow-up sessions (Burke and Gregoire, 2007).

vision' drug policy that seeks a drug-free society. The Swedes make no apologies for their compulsory treatment regime, viewing drug use as harmful to health that should not exist in a society that cares about its citizens (Swedish Drug Policy, 2016).⁹

Drug liberalisation advocates also argue that instead of drying up the drug supply and demand markets, drug prohibition stimulates the black market. The unregulated nature of the black market means that drug supply syndicates or cartels may manipulate the purity of the illicit substances (Coyne and Hall, 2017; Bell, 2010; Resignato, 2000; Hillam, 2004; Miron, 1985). For example, the purity of cocaine or heroin may be cut 5 times or even 20 times. Sugar or even rat poison could be added to lace it as a means of securing greater profit for the organised crime syndicates trafficking in such drugs. On the other hand, its purity may be used to ensnare new users (Coyne and Hall, 2017).

While this argument for transparency is on the face of it rational, one ought to note that the policy design and implementation would have unintended consequences. Quite plainly, policy experimentations can be irreversible, and can well result in adverse effects. There is no guarantee that black markets will not persist

alongside regulated markets. We see this happening for many regulated commodities, not least alcohol and tobacco where high taxes are slapped on (Thompson, 2014). Given that jurisdictions have imposed taxes on the sale of drugs to raise fiscal revenue, there may well be opportunities for organised crime to offer drugs at lower tax-free prices. In the case of psychoactive substances, their free supply would also open the floodgates to the growth of demand, and result in the consequent harms of addiction, crime and sexually transmitted diseases (Wang, Le Lait, Deakayne, Bronstein, Bajaj and Roosevelt, 2016).¹⁰ It is worthwhile to note that the legalisation of marijuana in several states of the US has reportedly moved drug cartels to push more potent substances like methamphetamine, heroin and fentanyl, an extremely powerful synthetic opioid into the country. This has fuelled an epidemic in the US – already in America are at their highest today (Tucker, 2017; Duffy and Baldwin, 2012). In the US alone, a total of 52,404 people died from drug overdose in 2015 (Rudd et al., 2016). This is higher than the 35,092 traffic accident deaths and 36,252 deaths by firearms recorded in the US that year (Centers for Disease Control and Prevention, 2016, 2017; National Highway Traffic Safety Administration, 2016). In England and Wales, a recent bulletin published by the UK Office for National Sta-

⁹ Sweden's national drug strategy includes legal provisions on compulsory care for substance abusers, whereby substance use disorders without the presence of psychoses or other severe mental disorders, may be grounds for compulsory commitment to care. This means that an individual may be placed in compulsory care without his or her consent if an administrative court finds it necessary in order to protect the individual and or others from physical, mental or social harm. (Reitan, 2016).

¹⁰ In Colorado, which legalised recreational use of cannabis in 2012, published reports using official statistics and federal surveys of drug use have stated no adverse effects on youths' propensity to smoke weed amongst Coloradans (Drug Policy Alliance, 2016; Ingraham, 2015). However, this was countered by reports published by the National Survey on Drug Use and Health by the Substance Abuse and Mental Health Services Administration, which showed an estimated increase in cannabis users in 2015 compared to earlier years (American College of Pediatricians, 2017). A study by JAMA Paediatrics also showed a deterioration in public health since legalisation, based on higher rates of hospital visits and cases at poison centres for unintentional paediatrics exposure to cannabis (Wang, Le Lait, Deakayne, Bronstein, Bajaj and Roosevelt, 2016).

tistics reported 3,744 registered “drug poisoning deaths” in 2016. The report also noted a sharp increase from 2012 to 2015 in drug misuse deaths.¹¹ The figure in 2016 was the highest number recorded since 1993: about 70% of the total “drug poisoning deaths” were due to “drug misuse” (UK Office for National Statistics, 2017).

‘War on Drugs’: Success or Failure?

The war on drugs that has dominated international drug control policy in the last four decades sought to reduce the supply of illicit drugs through tough legislation and active law enforcement. Nearly half a century after its advent, those with a casual attitude towards drugs have judged this approach a failure. They cite as evidence the overpopulation of prisons in many parts of the world with drug offenders and high drug addiction rates (Barnett, 2009; Jensen, Gerber and Mosher, 2004). Critics also draw parallels between the ‘war on drugs’ and America’s Prohibition Act (1920 to 1933) that engendered the growth of organised crime that made money from the manufacture, distribution, and sale of alcohol. There was also violence and murder among organised crime gangs, and corruption was rife among police officers and political officials who profited from organised crime. Furthermore, the criminal justice system spent an inordinate amount of time, money and energy to enforce the provisions of the Prohibition Act (Thompson, 2014).

It is worth noting that how the ‘war’ on drugs is assessed really boils down to the very definition of success and failure and to whom the question is posed. For example, while high rates

of incarceration in many parts of the world are perceived as an outcome of drug criminalisation, drug prohibitionists point out that the large number of people incarcerated are for concurrent criminal as well as drug-related offences (MacCoun, et. al, 2003; Powell, 2011; McBride, Vanderwaal and Terry-McElrath, 2001). This strong drug-crime relationship validates the necessity for punitive sanctions, to protect society from the harms brought on by a strong drug-crime nexus. Moreover, the assumption that crime rates will decrease if drug use is decriminalised or drugs are made freely available is purely speculative. Indeed, one could argue that falling crime rates are only possible if crimes committed by drug users seeking money to buy drugs, and the dealers protecting their rights to sell drugs, fall by an amount greater than the increase in crimes committed by existing and newly addicted users who are desperate for their fix but are economically emasculated because they are no longer capable of holding a job given their condition (Powell, 2011).

Conclusion

For a long time, the global community fought the scourge of drugs with almost a single voice. There was a global consensus on the immorality of drug use and the need to check supply. That consensus is now fracturing as advocates of a more liberal drug policy seek to discredit drug control by presenting arguments that appear reasonable, and even scientific. Yet, one should note that the evidence cited is often wanting, has been arbitrarily selected, and is often inapplicable in a broader context. Harm reduction proponents nowadays also tend to link their arguments to humanitarianism, con-

¹¹ Where the underlying cause is drug abuse or drug dependence, or a death where the underlying cause is drug poisoning and where any of the substances controlled under the Misuse of Drugs Act 1971 are involved.

trasting it to the allegedly repressive policies of their opponents. This has to be seen for the marketing tool it is. The case for humanitarianism can be made in many ways, including the argument that humanitarianism calls for a tough drug regime to protect individuals, their families and society against the harms of drug abuse. As harm reduction proponents who use the idea beyond its original intent and provenance and who pursue it as an end itself threaten our 'zero-drug' policy, they will have to be judiciously rebutted and exposed.

The task of advocacy against drugs involves

deconstructing their seemingly seductive arguments, exposing their false premises, and responding robustly to them with scientific and hard data evidence. In Singapore, the anti-drug endeavour employs a whole-of-government approach that works in partnership with the community and academia. These various agencies have been participating actively and in concert at various regional and international fora to defend Singapore's tough stance against drugs and its comprehensive approach. We will have to enhance these efforts even as we brace ourselves to meet the likely greater offensive that will come our way.

AODC in Action

Over the past year, Singapore government leaders and officials have taken part in international forums to advocate Singapore's position on drug control. AODC also worked with the Central Narcotics Bureau (CNB) and Singapore Prison Service (SPS) to organise seminars at home to familiarise public servants with the issues at stake and its impact on Singapore.

Meeting of ASEAN Senior Officials on Drug Matters (ASOD) 2016

The task of building a global coalition against attempts to liberalise the approaches to and policies on drugs and their use must begin with collaborating with our neighbours. Singapore is represented at the regional forums on drugs, and takes an active role in them. For example, at the ASEAN Senior Officials Meeting on Drug Matters (ASOD) held in August 2016, Benny Oon, who later assumed the post of Executive Director of AODC, shared his experiences at the UNGASS Outcome Document negotiations in early 2016 in Vienna, Austria. ASEAN diplomats were a unified voice in Vienna in the face of a contentious global setting and joined hands to ensure that language inimical to anti-drug efforts and drug policies in the region did not define the Outcome Document. Oon made the key point at ASOD that it was important for the various agencies and stakeholders of each country to work in concert and align their nation's policy positions on the issue of drug control. This ensured that a clear position on drugs control could be unequivocally expressed by the ASEAN delegates at various international fora, such as the Commission on Narcotic Drugs and World Health Assembly.

60th Session of the Commission on Narcotic Drugs (CND)

13 – 17 March 2017, Vienna, Austria

Singapore participated actively in the 60th edition of the Commission on Narcotic Drugs (CND). During the course of the annual meeting from 13-17 March 2017, AODC working in close collaboration with Singapore's Mission in Vienna and CNB, conceptualised and set up a thematic exhibition at the Vienna International Centre. The exhibition sought to highlight the Preventive Drug Education (PDE) aspects of Singapore's Drug Prevention policy as part of narrating the Singapore Story to an international audience. It allowed international visitors to have a holistic perspective of Singapore's preventive efforts, including our use of innovative methods to reach out to youths in partnership with the community.

ASEAN states and like-minded countries attending the 60th CND showed support for Singapore's PDE exhibition by attending the launch in good numbers. In the course of the reception, then Senior Minister of State for Home Affairs and National Development (and former Second Minister for Home Affairs) Desmond Lee engaged various Heads of Delegations as well as Non-Governmental Organisations that were supportive of Singapore's 'Harm Prevention' approach.



ASEAN Heads of Delegation posing in the classic 'ASEAN handshake' at the lunchtime reception hosted by Singapore.



Exhibition Panels on Singapore's Preventive Drug Education set up at the Rotunda, Vienna International Centre.

Seminar on Drug Prevention

AODC coordinated Singapore's participation for the first time at a CND side-event on the theme of Drug Prevention led by the United Nations Office on Drugs and Crime (UNODC). The Ministry of Home Affairs' Deputy Secretary International, T. Raja Kumar presented Singapore's unique brand of prevention efforts and successes through Preventive Drug Education activities. This focus on Drug Prevention enabled us to establish common ground with countries such as France, Norway and Iceland, despite their having different national approaches and policy positions on drug matters.



DS T. Raja Kumar presenting on Singapore's PDE efforts at the CND side event.



DS T. Raja Kumar with Chairman of the 60th Commission on Narcotic Drugs, Bente Angell-Hansen.

Seminar on Singapore's National Drug Control Policy for Public Service Officers, 30 June 2017

Even as we advocate on the international scene, we are working on alerting our domestic stakeholders to the new trend of decriminalisation and even legalisation of drug use that is sweeping across the world and the need for us to continue to be strongly anchored by our fundamentals in drug policy. AODC led a working group comprising officers from Central Narcotics Bureau, Singapore Prison Service and the Institute of Safety and Security Studies in this endeavour to develop a series of programmes reaching out to key identified constituencies in Singapore as part of this national drug advocacy outreach effort, which DS T. Raja Kumar actively guided.

The working group rolled out the first in this series of outreach programmes on 30 June 2017 to officers from key ministries in the public sector. The inaugural Seminar on Singapore's National Drug Control Policy for Public Service Officers was a flagship programme developed to reach out to officers from various ministries such as the Ministries of Foreign Affairs (MFA), Social and Family Development (MSF), Communication and Information (MCI), Health (MOH) and Home Affairs (MHA), who in their line of work will need to be well-versed with and equipped to explain and defend Singapore's drug policy positions domestically and internationally. The programme aimed to provide participants with a comprehensive understanding of Singapore's National Drug Control Policy through carefully curated content delivered in a storyline format, covering topics ranging from the history of drug abuse in Singapore, current challenges on the domestic and international fronts, Singapore's scientific and evidence-based rehabilitation efforts, and the deception behind arguments for decriminalisation and legalisation of



Seminar participants having a heart-to-heart sharing session with drug desistors.

certain types of drugs.

The seminar also included a visit to the Helping Hand Halfway House. The visit provided participants with a good insight into the real problems faced by drugs addicts through briefings, walk-about and a discussion session with former drug addicts. A fireside chat with Parliamentary Secretary for Home Affairs and Health, Amrin Amin, allowed the participants to get personal insights from the perspective of a political office holder tasked with drug policy development and implementation. Parl Sec Amrin explained to the participants the various avenues available for the differentiated rehabilitation of different segments of society, such as youths and adults, and dispelled commonly-held misconceptions relating to the death penalty for drug offences. The effectiveness of the seminar was captured in the programme survey responses, which registered increases in participants' knowledge and understanding of Singapore's national drug policies at the end of the course.



Fireside Chat with Parliamentary Secretary for Home Affairs & Health, Amrin Amin.



Former Second Minister Desmond Lee (left) sharing CNB's PDE with Executive Director of UNODC, Yury Fedetov.



Former 2PS (Home Affairs) Loh Ngai Seng addressing the participants.



Former Second Minister Desmond Lee speaking with the Myanmar Police Chief.



Prof Stella Quah presenting on Harm Reduction & Drug Addiction.



Fireside chat with Parliamentary Secretary for Home Affairs & Health, Amrin Amin.



Dr Jimmy Lee presenting on Medical Cannabis.



Director Communications Central Narcotics Bureau Sng Chern Hong presenting on 'History of Drug Abuse in Singapore'.



Director Central Narcotics Bureau Ng Ser Song opening the seminar.



Executive Director of Advocacy Office on Drugs and Crime Benny Oon discussing 'Current Reality - International Developments'.



Director Psychological and Correctional Rehabilitation Division Singapore Prisons Service, Timothy Leo presenting on 'Evidence-Based Approaches to Correctional Rehabilitation'.



Seminar participants having a heart-to-heart sharing session with drug desistors.



CEO of the Helping Hand Halfway House, Chia Shih Sheung, sharing his work with former drug addicts.

About the Authors

The Advocacy Office against Drugs and Crime (AODC) is helmed by Executive Director, Dr. Rozlan Giri, and Assistant Directors Sivaraman Letchumanan and Nur Asyikin Hamzah. AODC serves to secure Singapore's policy and operational space on drug matters through advocacy and training.

Dr. Rozlan Giri is concurrently Counsellor (UN), Permanent Mission of the Republic of Singapore, United Nations Office and Other International Organisations in Vienna. He holds a PhD from King's College, London and an MBA. He began his career in the Singapore Police Force where he assumed a wide range of postings in the staff, command and operational domains. He had also undertaken research relating to counter-terrorism at the Ministry of Home Affairs and at the S. Rajaratnam School of International Studies, Nanyang Technological University. In the course of his stint in the civil service, he was seconded to the Ministry of Education as the Deputy Chief Executive Officer of the Council for Private Education, MOE and the Chief Executive Officer of Yayasan Mendaki.

Sivaraman Letchumanan has been with the Advocacy Office against Drugs & Crime (AODC) since 2017. He joined the Senior Narcotics Service of the Central Narcotics Bureau in 1999 and has worked in areas of field operations, intelligence, investigation and corporate communications.

Nur Asyikin Hamzah joined AODC in July 2017. Prior to this, she was with the Singapore Prison Service since 2010, as a Correctional Rehabilitation Specialist with the Psychological & Correctional Rehabilitation Division. Nur Asyikin has worked in areas of correctional rehabilitation research and evaluation, and has provided counselling for the Reformative Trainees and the women offender populations. She is a Certified Substance Abuse Counsellor (CSAC) with the Association of Professionals Specialising in Addiction Counselling (APSAC), and has a Master in Counselling degree from Monash University.



References

- Advisory Council on the Misuse of Drugs. (1988). *AIDS and Drug Misuse: Part 1*. London: HMSO
- Ahern, J., Stuber, J., and Galea, S. (2007). Stigma, Discrimination, and the Health of Illicit Drug Users. *Drugs and Alcohol Dependence*, 88:188.
- American College of Pediatricians. (2017, February). Effect of Marijuana Legalization on Risky Behaviour. Retrieved from <http://www.acped.org/the-college-speaks/position-statements/effect-of-marijuana-legalization-on-risky-behavior>
- American Society of International Law. (1911, April). The International Opium Conference. *The American Journal of International Law*, 5(2), 466-472.
- Bai, N. (2011, March 4). Can You Cure Yourself of Drug Addiction? *Scientific American*. Retrieved from <http://www.scientificamerican.com/article/can-you-cure-yourself-of-addiction>
- Barnett, R.E. (2009). The Harmful Side Effects of Drug Prohibition. Georgetown University Law Center: *Scholarship @ Georgetown Law*. Retrieved from <http://scholarship.law.georgetown.edu/facpub>
- BBC: Canada Unveils Plans to Legalise Recreational Marijuana. (2017, April 13). Retrieved from <https://www.bbc.com/news/world-us-canada-39569993>
- Bell, J. (2010). The Global Diversion of Pharmaceutical Drugs: Opiate Treatment and the Diversion of Pharmaceutical Opiates – a Clinician’s Perspective. *Addiction*, 105(9): 1531-7.
- Bewley-Taylor, D.R. (2012). *International Drug Control: Consensus Fractured*. Cambridge University Press.
- Black, D.W. (2016). What Causes Antisocial Personality Disorder? *Psych Central*. Retrieved on September 18, 2017, from <https://psychcentral.com/lib/what-causes-antisocial-personality-disorder/>
- Brecht, M.L., Anglin, M.D., and Wang, J.C. (2009). Treatment Effectiveness for Legally Coerced Versus Voluntary Methadone Maintenance Clients. *The American Journal of Drug and Alcohol Abuse*, 19(1), 89-106.
- Bridge, J., Hunter, B.M., Atun, R., and Lazarus, J.V. (2012). Global Fund Investments in harm reduction from 2002 to 2009. *International Journal of Drug Policy*. 23: 279-285.
- Bonello, D. (2015, November 4). Mexico Ruling on Personal Marijuana Use for 4 Hailed by Legalization Backers. *Los Angeles Times*. Retrieved from <https://www.latimes.com/world/mexico-americas/la-fg-mexico-marijuana-20151104-story,amp.html>
- The Economist. (2009, August 27). Treating, Not Punishing. *The Economist*. Retrieved from <http://www.economist.com/node/14309861>
- Burke, A.C. and Gregoire T.K. (2007). Substance Abuse Treatment Outcomes for Coerced and Non-coerced Clients. *Health and Social Work*, 31: 7-15.
- Central Narcotics Bureau. (2016, June 20). Drug Situation Report. Retrieved from <http://www.cnb.gov.sg/drugsituationreport/drugsituationreport2016.aspx>
- Center for Disease Control and Prevention. (2017). WISQARS Fatal Injury Reports. Retrieved from: <https://www.webappa.cdc.gov/sasweb/ncipc/mortrate.html>
- Coyne, C.J. and Hall, A.R. (2017). *Four Decades and Counting: The Continued Failure of the War on Drugs*. Washington DC: CATO Institute.
- Crisp, B.R. and Barber, J.G. (1997). The Prevention of AIDS Among Injecting Drug Users. *British Journal of Social Work* 272: 255-274.
- Domoslowski, A. (2011, June). Drug Policy in Portugal: The Benefits of Decriminalizing Drug Use, Open Society Foundations, Global Drug Policy Program, New York. Retrieved from <http://www.opensocietyfoundations.org/sites/default/files/drug-policy-in-portugal-english-20120814.pdf>
- Dorabjee, J. (2015). The View from the Trenches. *Harm Reduction Journal* 12: 44.
- Duncan, D.F. and Nicholson, T. (1997). Dutch Drug Policy: A Model for America? *Journal of Health Social Policy* 8(3): 1-15.

- Drug Policy Alliance. (2016, October 13). So Far, So Good: What We Know about Marijuana Legalization in Colorado, Washington, Alaska, Oregon and Washington D.C. Retrieved from http://drugpolicy.org/sites/default/files/Marijuana_Legalization_Status_Report_101316.pdf
- Duffy, P. and Baldwin, H. (2012). The Nature of Methadone Diversion in England: A Merseyside Case Study. *Harm Reduction Journal* 9:3.
- Erikson, P.G., Riley, D.M., Cheung, Y.W., O'Hare, P.A. (1997). *Harm Reduction: A New Direction for Drug Policies and Programs*. Toronto: University of Toronto Press.
- Felix, S., and Portugal, P. (2017). Drug Decriminalization and the Price of Illicit Drugs. *International Journal of Drug Policy*, 39, 121-129.
- The European Monitoring Centre for Drugs and Drug Addiction (EMCDDA). (2001). Decriminalisation in Europe: Recent Developments in Legal Approaches to Drug Use. Retrieved from http://eldd.emcdda.org/databases/eldd_comparatuce_analyses.cfm
- Ginexi, E.M., Foss, M.A., Scott, C.K. (2003). Transitions from Treatment to Work: Employment Patterns Following Publically Funded Substance Abuse Treatment. *Journal on Drug Issues* 33: 497-518.
- Goodle, F. and Hurley, R. (2016). The War On Drugs Has Failed: Doctors Should Lead Calls for Drug Policy Reform. *British Medical Journal* 355:16067. Retrieved from <https://doi.org/10.1136/bmj.i6067>
- Government.se. (2016, April 11). Swedish Drug Policy – A Balanced Policy Based on Health and Human Rights. Retrieved from http://www.government.se/496f5b/contentassets/89b85401ed204484832fb1808cad6012/rk_21164_broschyr_narkotika_a4_en_3_tillg.pdf on 8 November 2017.
- Greenwald, G. (2009). *Drug Decriminalization in Portugal: Lessons in Creating Fair and Successful Drug Policies*. Washington DC: CATO Institute.
- Harm Reduction Australia (2015). What is Harm Reduction? Retrieved from <https://harmreductionaustralia.org.au/what-is-harm-reduction/>
- Heather, N., Wodak, A., Nadelmann, E., and O'Hare, P., Eds. (1993). *Psychoactive Drugs and Harm Reduction: From Faith to Science*. London: Whurr.
- Hoffman R.S., and Goldfrank L.R. (1990). The Impact of Drug Abuse and Addiction on Society. *Emergency Medicine Clinics of North America* 8(3):467-80.
- Hillam, L. (2004). Alcohol and Temperance in Modern History: An International Encyclopaedia, *Reference Reviews*, Vol. 18 Issue 6, pp.18-19.
- Hughes, C.E. and Stevens, A. (2012). A Resounding Success or a Disastrous Failure: Re-Examining the Interpretation of Evidence on the Portuguese Decriminalization of Illicit Drugs. *Drugs and Alcohol Review* 31: 101-113.
- Hughes, C.E. and Stevens, A. (2010). What Can We Learn From the Portuguese Decriminalization of Illicit Drugs? *British Journal of Criminology*, 50: 999-1022.
- Hughes, C. and Stevens, A. (2007). The Effects of Decriminalization of Drug Use in Portugal. The Beckley Foundation. United Kingdom, Beckley Foundation Briefing Papers
- Ingraham, C. (2015, December 18). Legal Weed Having Little Effect On Teen Marijuana Use, Federal Data Shows. Wonkblog. Retrieved from http://www.washingtonpost.com/news/wonk/wp/2015/12/18/legal-weed-having-little-effect-on-teen-marijuana-use-federal-data-shows/?utm_term=.bb772c185f67
- International Harm Prevention Association. (2010). What is Harm Reduction? A Position Statement from the International Reduction Association. Retrieved from [www.ihra.net/files/2010/09/10/BriefingWhat isHREnglish.pdf](http://www.ihra.net/files/2010/09/10/BriefingWhat%20isHREnglish.pdf)
- Jason, L., Davis, M., Ferrari, J., and Bishop, P. (2001). Oxford House: A Review of Research and Implications for Substance Abuse Recovery and Community Research. *Journal of Drug Education* 31(1), 1-27.
- Jakubiec, D., Kilcer, A., Sager, W. (2009). The War on Drugs. RIT: College of Liberal Arts 2009. Retrieved from <http://scholarworks.rit.edu/article/1662>.
- Jensen, E.L., Gerber, J., and Mosher, C. (2004). Social Consequences of the War on Drugs: The Legacy of Failed Policy. *Criminal Justice Policy Review*, 15, (1): 100-121.
- Kinderman, P. (2009). Understanding and Addressing Psychological and Social Problems: The Mediating Psycho-

- logical Processes Model. *International Journal of Social Psychiatry* 55(5): 464-470.
- Lande, A. (1962). The Single Convention on Narcotic Drugs, 1961. *International Organization* 16(4), 776-797.
- Landar, L., Howsare, J, and Byrne, M. (2013). The Impact of Substance Use Disorders on Families and Children: From Theory to Practice. *Social Work Public Health*. 28(0): 194-205.
- Laqueur, H. (2015). Uses and Abuses of Drug Decriminalization in Portugal. *Law & Social Inquiry* 40(3): 716-781.
- Levine, H.G. (2002). The Secret of Worldwide Drug Prohibition. *The Independent Review* 7: 165-80.
- MacCoun, R.J. (1998). Toward a Psychology of Harm Reduction. *American Psychologist* 53(11): 1199-1208.
- MacCoun, R.J., Kahan, J. Gillespie, J., and Rhee, J. (1993). A Content Analysis of the Drug Legalization Debate. *Journal of Drug Issues* 23, 615-629.
- McBride, D., VanderWaal, C., and Terry-McElrath, Y. (2001). The Drugs-Crime Wars: Past, Present, and Future Directions in Theory, Policy and Program Interventions. *The National Institute of Justice*.
- Michels, I.I., Stover, H., and Gerlach, R. (2007). Substitution Treatment for Opioid Addicts in Germany. *Harm Reduction Journal* 4:5
- McKeganey, N. (2011). From Harm Reduction to Drug User Abstinence: A Journey in Drug Treatment Policy. *Journal of Substance Use*, 16(3): 179-194.
- McKeganey, N., Bloor, M., Robertson, M., Neale, J. and MacDougall, J. (2006). Abstinence and Drug Abuse Treatment: Results from the Drug Outcome Research in Scotland Student. *Drugs: Education, Prevention & Policy*, 13(6).
- McKeganey, N. (2004). What are Drug Users Looking for When They Contact Drug Services: Abstinence or Harm Reduction? *Drugs: Education, Prevention and Policy*, Vol 11(5): 423-435.
- Miller N.S. Flaherty, J.A. (2000). Effectiveness of Coerced Addiction Treatment (Alternative Consequences): A Review of the Clinical Research. *Journal of Substance Abuse Treat*, 18(1): 9-16.
- Mosher, J.F., and Yanagisako, K.L. (1991). Public Health, Not Social Warfare: A Public Health Approach to Illegal Drug Policy. *Journal of Public Health Policy* 12(3): 278-323.
- Narayanan, S., Vicknasingam, B., and Md. Haris Robson, N. (2011). The Transition to Harm Reduction: Understanding the Role of Non-Governmental Organisations in Malaysia. *International Journal of Drug Policy* 22: 311-317.
- National Treatment Agency, (2008). Annual Report 2007-2008.
- National Council against Drug Abuse (NCADA). (2017, April 27). Youths Display More Liberal Views Towards Drugs; Parental Influence Key in Deterring Drug Abuse [News Release]. Singapore.
- National Highway Traffic Safety Administration (NHTSA). (2016, August 29). Traffic Fatalities Up Sharply in 2015. Retrieved from: <https://www.nhtsa.gov/press-releases/traffic-fatalities-sharply-2015>
- National Institute of Drug Abuse (NIDA). (2017, January 6). Overdose Death Rates. Retrieved from <https://www.drugabuse.gov/related-topics/trends-statistics/overdose-death-rates> on August 6, 2017.
- National Institute of Drug Abuse (NIDA). (2014, July 1). Drugs, Brains, and Behavior: The Science of Addiction. Retrieved from <https://www.drugabuse.gov/publications/drugs-brains-behavior-science-addiction> on 2017 on August 1, 2017.
- Neale, J. (2004). Gender and Illicit Drug Use. *British Journal of Social Work*, 34, 851-870.
- Nutt, D. (2012). *Drugs without the Hot Air: Minimizing the Harms of Legal and Illegal Drugs*. UIT Cambridge.
- Office of National Drug Control Policy (ONDCP). (2011, February 24). Reconsidering the decriminalization of drugs in Portugal. Retrieved from <http://www.wfad.se/images/articles/ondcp%20portugal.pdf>
- Office of National Drug Control Policy. (2000). The National Drug Control Strategy. Washington, D.C.: Office of National Drug Control Policy, Executive Office of the President.
- O'Hare, P. (2007). Merseyside, the First Harm Reduction Conferences, and the Early History of Harm Reduction. *The International Journal of Drug Policy* 18(2): 141-144.
- Palamer, J.J., Kiang, M.V., and Halkitis, P.N., (2012). Predictors of Stigmatization Towards Use of Various Illicit Drugs Among Emerging Adults. *Journal of Psychoactive Drugs* 44(3): 243-51.

- Perron, B.E. and Bright, C.L. (2008). The Influence of Legal Coercion on Dropout from Substance Abuse Treatment: Results from a National Survey. *Drug Alcohol Dependence*, 92(1-3): 123-131.
- Pinto Coelho, M. (2010). The 'resounding success' of Portuguese drug policy: the power of an attractive fallacy. Lisboa: Associação para uma Portugal livre de drogas.
- Pinto Coelho, M. Britain Should Not Make the Same Mistakes as Portugal (Stockholm: World Federation Against Drugs, 2010). October 2. Retrieved from <http://wfad.se/latest-news/1-articles/365-britain-should-not-make-the-same-mistakes-as-portugal> on 2017, September 18.
- Powell, M.A. (2011). A Comprehensive Analysis of the Drug-Crime Relationship. Research Papers. Paper 100. Retrieved from http://opensiuc.lib.siu.edu/gs_rp/100/
- Quah, Stella R. (2017). Illicit Psychoactive Substance Use and Harm Prevention. *International Encyclopedia of Public Health* (2):157-181
- Quello, S.B., Brady, K.T., and Sonne, S.C. (2005). Mood Disorders and Substance Use Disorder: A Complex Comorbidity. *Science & Practice Perspectives*, 3(1): 13-21.
- Rahman, F. and Crofts, N. (2013). *Drug Law Reform in East and Southeast Asia*. Lexington Books.
- Reinarman, C. and Levine, H.G. (1997). 'Real Opposition, Real Alternatives: Reducing the Harms of Drug Use and Drug Policy', in Reinarman, C. and Levine, H.G. (eds.), *Crack in America: Demon Drugs and Social Justice*. University of California Press, p. 355.
- Reitan, T. (2016). Commitment Without Confinement: Outpatient Compulsory Care for Substance Abuse, and Severe Mental Disorder in Sweden. *International Journal of Law and Psychiatry*, 45: 60-69.
- Riley, D. and O'Hare, P., 'Harm Reduction: History, Definition and Practice,' in Inciardi, J.A. and Harrison, L.D. (eds.), *Harm Reduction: National and International Perspectives* (London, Thousand Oaks: Sage, 2000), p.2.
- Rivera, B., Casal, B., Currais, L. (2017). The Social Cost of Illicit Drug Use in Spain. *International Journal of Drug Policy*, 44: 92-104.
- Robert, L. (2005). Is the War on Drugs Succeeding? *Harvard Law Bulletin*. Retrieved from <http://today.law.harvard.edu/feature/war-drugs-succeeding/>
- Roe, G. (2005). 'Harm Reduction as Paradigm: Is Better than Bad Good Enough? The Origins of Harm Reduction', *Critical Public Health*, 15, 3: 243-50.
- Rosemarin, A., and Eastwood, N. (2012). A Quiet Revolution: Drug Decriminalization Policies in Practice Across the Globe. *New York: Open Society Foundations*: 1-42.
- Rudd, R., Seth, P., David, F., and Scholl, L. (2016). Increases in Drug and Opioid-Involved Overdose Deaths – United States, 2010-2015. *MMWR Morb Mortal Wkly*. Retrieved from <https://www.cdc.gov/mmwr/65051e1.htm>
- Santamaria, J. (2000). *Drugs Dilemma: A Way Forward*. Australia: New Weekly Books.
- Scientific American (April 7, 2009). 5 Years After: Portugal's Drug Decriminalization Policy Shows Positive Results. *Scientific American*. Retrieved from <http://www.scientificamerican.com/article/portugal-drug-decriminalization/>
- Sterling, R.C., Gotheil, E., Glassman, S.D., Weinstein, S.P., Serota, R.D., Lundy, A. (2001). Correlates of Employment: A Cohort Study. *The American Journal of Drug and Alcohol Abuse* 27: 137-146.
- Substance Abuse and Mental Health Services Administration. (2004). Overview of Findings from the 2003 National Survey on Drug Use and Health. Office of Applied Studies, NHSDA Series H-24, DHHS Publication No. SMA 04-3963, Rockville, MD.
- Single, E., Christie, P., & Ali, R. (2000). The Impact of Cannabis Decriminalisation in Australia and the United States, *Journal of Public Health Policy* 21(2):168.
- Stevens, A. (2011). Drug Policy, Harm and Human Rights: A Rationalist Approach. *International Journal of Drug Policy* 22(3): 233-8.
- Stimson, G.V. (1995). AIDS and Injecting Drug User in the United Kingdom, 1988-1993. *Social Science and Medicine* 41: 699-716.
- Stimson, G.V. (1990). AIDS and HIV Challenge for British Drug Policy. *British Journal of Addiction*, 85, 329-339.

- Tammi, T. and Hurme, T. (2007). 'How the Harm Reduction Movement Contrasts Itself Against Punitive Prohibition', *International Journal of Drug Policy*, 18, 2: 84–7.
- Tammi, T. (2004). The Harm Reduction School of Thought: Three Fractions. *Contemporary Drug Problems* 31(3), 381-399.
- TIME. (2009, April 26). Drugs in Portugal: Did Decriminalization Work? *TIME*. Retrieved from <http://content.time.com/time/health/article/0,8599,1893946,00.html>
- The Economist. (2009, August 27). Treating, Not Punishing. *The Economist*. Retrieved from <http://www.economist.com/node/14309861>
- Thompson, G.O. (2014). Slowly Learning the Hard Way: U.S. America's War on Drugs and Implications on Mexico. *Norteamerica, Year 9, Issue 2*, July-December 2014, 59-83.
- Tucker, D. (2017, July 5). Mexico Most-Wanted: A Guide to the Drug Cartels. *BBC*. Retrieved from <https://www.bbc.com/news/amp/world-latin-america-40480405>
- United Nations. (2015, May 7). War on Drugs 'Painstaking, Often Thankless, Seemingly Unending' Struggle, General Assembly Hears in Thematic Debate Laying Ground for New Global Approach. [Press release]. Retrieved from <https://www.un.org/press/en/2015/ga11642.doc.htm> on August 1, 2017.
- United Nations. (1961). Single Convention on Narcotic Drugs, 1961, As Amended by the 1972 Protocol Amending the Single Convention on Narcotic Drugs 1961. Retrieved from http://www.unodc.org/pdf/convention_1961_en.pdf
- United Nations. (1971). Convention of Psychotropic Substances, 1971. Retrieved from http://www.unodc.org/pdf/convention_1971_en.pdf
- United Nations. (1988). Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988. Retrieved from http://www.unodc.org/pdf/convention_1988_en.pdf
- United Nations International Drug Control Programme, United Nations Office for Drug Control and Crime Prevention, and United Nations Office on Drugs and Crime. (2006). *World Drug Report*. Oxford: Oxford University Press.
- United Nations, General Assembly, Outcome Document of the 2016 United Nations General Assembly Special Session on the World Drug Problem – Our Joint Commitment to Effectively Addressing and Countering the World Drug Problem. 2016, April 19-21). Retrieved from <https://www.unodc.org/documents/postungass2016/outcome/V1603301-E.pdf>
- Vastag, B. (2009, April 7). 5 Years After: Portugal's Drug Decriminalization Policy Shows Positive Results. *Scientific American*. Retrieved from <https://www.scientificamerican.com/article/portugal-drug-decriminalization/>
- Wang, G.S., Le Lait, M., Deakayne, S.J., Bronstein, A.C., Bajaj, L., and Roosevelt, G. (2016). Unintentional Pediatric Exposures to Marijuana in Colorado, 2009-2015. *JAMA Pediatr.* 2016; 170 (9).
- Whitesell, M., Bachand, A., Peel, J., and Brown, M. (2013). Familial, Social, and Individual Factors Contributing to Risk for Adolescent Substance Use: *Journal of Addiction*.
- Wodak, A. (1999). What is this thing called Harm Reduction? *International Journal of Drug Policy* 10: 169-71.

Empowering The Community Against Terrorism

EVOLUTION OF THE TERRORISM THREAT TO SINGAPORE

By Counter-Terrorism Division
Internal Security Department

The terrorist threat to Singapore is not new. But as it evolves, so too must Singapore's counter-terrorism efforts, a key component of which has always been to prepare the people through community engagement activities. The first article in this section provides a historical overview and current assessment of the terrorist threat Singapore faces while the second explains why a new national movement is now needed to sensitise, organise, train and exercise Singaporeans to better protect themselves from a terrorist attack.

For a younger generation of Singaporeans, the notion of terrorism perhaps first hit home when the September 11, 2001 attacks took place in the United States, followed by the discovery of the Jemaah Islamiyah (JI) network in Singapore. What is less known is that Singapore's brush with terrorism began much earlier with the Communist insurgency in Malaya in the 1940s, continuing with assassination attempts and other acts of violence in Singapore up till the 1970s. Singapore also suffered several terrorist attacks during Konfrontasi, including the MacDonald House bombing in 1965.

In post-Independence Singapore, we had the "Laju" incident where members of the Japanese Red Army and Popular Front for the Liberation of Palestine staged an attack on the Shell oil refinery complex on Pulau Bukom and hijacked the "Laju" ferryboat in January 1974. In 1985 and 1986, we saw small bomb explosions at Faber House along Orchard Road. We believe the target was the Israeli embassy that had an office space in Faber House at the time. In 1991, four Pakistani terrorists hijacked Singapore Airlines shuttle flight SQ 117 minutes after take-off from Kuala Lumpur. Our secu-

rity forces eventually killed the four hijackers. In these terrorist incidents, Singapore was not the target. The targets were third countries and the perpetrators were foreigners.

Then came the 9/11 attacks, which was a game-changer in terms of how countries defined and dealt with the threat of transnational terrorism. The scale of the simultaneous attacks was unprecedented, and focused the counter-terrorism (CT) spotlight on the threat posed by global jihadist terrorism, whose cause is actively championed by Al-Qaeda (AQ) and like-minded terrorist groups. 9/11 forced a necessary re-think for security agencies in terms of counter-terrorism efforts, and for Singapore, this came sooner than expected with the discovery of the JI network in December 2001, three months after 9/11. This time Singapore was the target and the JI members were Singaporeans.

More than a decade after 9/11 and the JI discovery, Singapore remains vulnerable to the threat of terrorism, which continues to evolve. Developments in the Middle East, underlined by the emergence of the Islamic State in Iraq and Syria (ISIS) and the increasing threat posed by self-radicalised individuals, have heightened the terrorism threat that we face today.

Jemaah Islamiyah:

Beginning of Singapore's Experience with Jihadist Terrorism

Singapore's experience with jihadist terrorism first began with the discovery of the local JI network in 2001. Some JI members had participated in the Soviet-Afghan war, where they forged links with AQ members and other militants, including those from the Moro Islamic Liberation Front (MILF). The sinister implications of the links forged between local JI members and AQ elements in Afghanistan became

evident when we uncovered the joint AQ-JI plots to carry out terrorist attacks on targets in Singapore. The most developed of these plots was the plan to mount multiple truck-bomb suicide attacks against the US and Israeli embassies. The Australian and British High Commissions were also identified as targets due to their proximity to the US embassy. The Singapore JI had also apprised AQ of its plan to carry out an attack against a regular shuttle bus service carrying US military personnel between Sembawang Wharf and Yishun MRT station. JI members of these operation cells produced observation reports and video-recordings of the reconnaissance conducted. A copy of the videotape of the reconnaissance of Yishun MRT station was subsequently conveyed to an AQ member in Afghanistan. Separately, JI members had also filmed US warships in the Straits of Johor for the purpose of targeting them using an explosives-laden boat.

Apart from the above plots that were developed in collaboration with AQ, the local JI network also made other preparations for terrorist attacks against selected Singapore targets, including:

- Water pipelines and waterworks stations
- Changi Airport and the nearby radar station
- Ministry of Defence Headquarters
- Jurong Island (where a number of petrochemical plants are located)
- MRT stations including the Operations Control Centre
- Ministry of Education headquarters

The purpose of targeting key installations like water pipelines was to create chaos in Singapore and Malaysia. The plan was to make the attacks appear as if they were acts of aggression by the Malaysian government. This would create an atmosphere of distrust and animosity between the two countries, which JI intended to portray as a 'Chinese Singapore'

threatening Muslims in Malaysia. Playing the race and religion card, JI would unleash ethnic conflict and civil strife through jihad. JI would then take advantage of the chaotic and revolutionary situation in Malaysia to overthrow the Malaysian government and establish an Islamic State comprising Malaysia and Singapore.

The Singapore JI was severely disrupted by two security operations in 2001 and 2002. Singapore JI members were arrested and subsequently dealt with under the Internal Security Act (ISA). Several who fled Singapore to evade capture were tracked down and captured with the assistance of regional authorities. They were similarly dealt with under the ISA upon their return to Singapore.

Current Terrorism Threat Facing Singapore: Serious, Diverse & More Challenging

Unfortunately, the terrorism threat against Singapore did not abate with the disruption of the Singapore JI. In fact, the terrorism threat confronting Singapore today is at its highest since the AQ-JI plots were disrupted in 2001. The tempo of terror-related activities in Southeast Asia has picked up, especially over the past two years, fuelled largely by developments in Syria and Iraq. Specifically, ISIS and its narrative of an 'Islamic Caliphate' have found strong support within jihadist communities in our region; many individuals have also been radicalised by ISIS's extremist ideology. At the same time, AQ, which has been consolidating its strength in areas of weak governance like Yemen and the Sahel (in Africa), has shown indications of renewed interest in Southeast Asia. There are also reports that the regional JI has rebuilt its network.

Security threat from ISIS

ISIS is the first jihadist terrorist group to have

succeeded in controlling substantial territory; its proclamation of the 'Islamic Caliphate' in June 2014 gave it an aura of divine sanction and enabled it to inspire and recruit thousands across the world. With its mastery of social media tools and platforms, ISIS's global influence far exceeds that of any other terrorist group, including AQ. While Southeast Asia is geographically removed from the conflict zone in Syria and Iraq, it is not immune to the terrorist threat that ISIS presents. As many as 1,000 Southeast Asians have joined the conflict in Syria and Iraq, variously fighting for groups like ISIS and AQ. Several regional militant groups have pledged allegiance to ISIS leader, Abu Bakr al-Baghdadi.

Since late 2015, ISIS has faced significant setbacks in the Syria/Iraq conflict zone, including the loss of key leaders, thousands of fighters, territories and sources of funding. However, these setbacks have also prompted ISIS to redouble efforts to expand the battleground beyond Syria/Iraq, into countries opposed to ISIS.

The nature of foreign terrorist operations conducted in the name of ISIS can be classified into three broad categories. On one level, ISIS-directed terrorist cells have conducted sophisticated attacks involving firearms and improvised explosive devices (IEDs) – examples include the Paris attacks in November 2015, Brussels bombings in March 2016 and Dhaka attack in July 2016. On another level, ISIS has endorsed or suggested attacks by individuals who have been in touch with the group, offering approval, guidance and encouragement either online or via an encrypted messaging service. The Jakarta attack in January 2016 could be considered to be such an attack. On a third level, pro-ISIS radical groups or radicalised individuals respond to calls by ISIS to mount attacks in their homelands; often, their weapon is anything at their disposal,

like knives and vehicles.

ISIS has been linked to several attacks and plots across Southeast Asia. In August 2016, Indonesian authorities arrested several ISIS-linked terrorists in Batam for involvement in a plot to mount a rocket attack against Singapore, targeting Marina Bay Sands. The suspects reportedly belonged to a terrorist cell, Katibah Gonggong Rebus, which had received instructions from Bahrun Naim, a Syria-based Indonesian member of ISIS.

As ISIS loses ground in the Syria/Iraq conflict zone, ISIS fighters from Southeast Asia may return to this region, possibly accompanied by other ISIS foreign fighters. In September 2016, it was reported that ISIS had trained 400 to 600 fighters for 'external operations' (beyond the conflict zone) involving urban guerrilla warfare and IEDs.¹ It is conceivable that returnee ISIS fighters might be tasked to conduct attacks in Southeast Asia, just as returnee ISIS fighters were involved in the 2015 Paris and 2016 Brussels attacks.

ISIS had, in November 2014, declared its intention to set up a wilayat (province) in Southeast Asia. To this end, southern Philippines has emerged as the epicentre of ISIS's violent campaign. On 23 May 2017, pro-ISIS militants laid siege to Marawi City in southern Philippines. The violence in Marawi, which dragged on for over four months, has serious repercussions for security in the region, including Singapore. ISIS can be expected to seek territorial expansion through the use of violence beyond southern Philippines. They could also call on fellow Muslims including those from Singa-

pore to travel to and engage in violence in other conflict zones.

Impact on Singapore

Singaporeans are not immune to the radicalising influence of ISIS propaganda. In 2013, two Singapore citizen, Haja Fakkurudeen Usman Ali and Maimunah binti Abdul Kadir made their way to Syria with their families to take part in the conflict there. They are believed to be still in Syria. In 2014, a third Singaporean, Megat Shahdan bin Abdul Samad, also travelled to Syria to join ISIS. He was recently featured in an ISIS propaganda video that is part of a series titled 'Inside the Caliphate'.

There has also been a sharp rise in the number of radicalised Singaporeans detected. Between 2007 and 2014, security actions were taken under the ISA against 11 individuals who were radicalised. In the two years since January 2015, the Singapore Government has taken security action against 17 others who were radicalised. Most of them had intended to fight alongside ISIS. Two had also been prepared to heed ISIS's call to carry out attacks on home-soil if they could not travel to Syria.

In recent years, we have also detected radicalised individuals among foreigners working in Singapore. Since 2015, nine foreign domestic workers in Singapore have been investigated for suspected radicalisation. Between November 2015 and April 2016, 40 radicalised Bangladeshi nationals were arrested. They supported the use of violence to pursue their extremist ideology and most planned to carry out armed jihad against the Bangladesh gov-

¹ Omar Ashour, The Islamic State's European strategy, Project Syndicate, 1 September 2016. Retrieved from <https://www.project-syndicate.org/commentary/islamic-state-european-strategy-by-omar-ashour-2016-09?barrier=accessreg>

ernment. While investigations did not reveal any attack plans against Singapore, we cannot be sure that they would not have attacked Singapore if ordered to do so or if the opportunity presented itself. Indeed, a group leader among the 40 arrested admitted that he would carry out attacks wherever directed by ISIS. Except for four who are currently serving sentences in Singapore for terrorism financing offences, the other Bangladeshi nationals have been repatriated to Bangladesh.

Threat Posed by JI and AQ

JI and AQ continue to pose a threat to Southeast Asia. JI is regrouping in Indonesia and membership size has increased to its pre-Bali 2002 attack numbers. Some JI factions have pledged allegiance to ISIS while others continue to align with AQ, which has also refocused its attention on Southeast Asia. In January 2016, AQ leader Ayman al-Zawahiri released an audio speech in which he urged Muslims in Indonesia, the Philippines, south Thailand, Ma-

laysia, and ‘what neighbours it’ – which could include Singapore – to contribute to jihad.

Conclusion

The global and regional terrorism landscape has evolved significantly since 2001. While groups like AQ and JI continue to pose a threat, ISIS together with the growing self-radicalisation phenomenon and ongoing conflict in Syria and Iraq have added to the threat. The terrorism threat facing us today is more diverse and in many ways, much harder to deal with. In order to confront the terrorism threat effectively and holistically, the different Home Team agencies, together with the members of the public, need to work together to forge a robust security chain that integrates intelligence, border security, policing of high-risk establishments and community vigilance.

About the Author

The article was contributed by ISD’s Research Command which has a team of officers involved in counter-terrorism research and investigations.

EMPOWERING THE COMMUNITY
BUILDING THE SGSECURE MOVEMENT:

A Transformation in our Counter-Terrorism Approach

By Tan Jin Rui Jerald
Community Partnership and Communications Group,
Ministry of Home Affairs

Why Do We Need a Transformation in Our Approach to the Terror Threat?

On 22 March 2017, a brazen terrorist attack took place right in the vicinity of the Palace of Westminster in London, a well-guarded location. The lone attacker, a 52-year old Briton named Khalid Masood, drove a car into pedestrians on the pavement, killing four and injuring fifty people in the process. He then proceeded to ram his car into the perimeter fence of the Palace grounds before abandoning it to run into the compound, where he fatally stabbed a police officer. He was subsequently shot and killed by another police officer.

The Westminster attack took place despite the fact that the UK's threat level for terrorism had been at 'Severe', the 2nd-highest level

in the UK scale, since August 2014¹. Despite the high level of security and alertness, a single terrorist was able to execute an attack at a prominent and tightly guarded location.

Indeed, there followed a series of attacks in the UK – the Manchester Arena bombing on 22 May 2017, the London Bridge attack on 4 June 2017, and most recently, the attack outside Finsbury Park Mosque on 19 June 2017. All these attacks occurred even while the UK maintained its 'Severe' threat level.

These attacks, along with many others around the globe, show us that the nature of the terror threat has changed and continues to evolve unpredictably. The rise of the Islamic State in Iraq and Syria (ISIS), coupled with the proliferation of the internet and social media², has

¹ Smith, Reiss (2017, March 22) UK terror threat level: What is the terror threat level in Britain and London? *The Express*. Retrieved from <https://www.express.co.uk/news/uk/695427/terror-threat-uk-level-britain-how-likely-attack-isis-islamic-state-london>

² Chan, Anton. (2015, May). The Call of ISIS: The Medium and the Message Attracting Southeast Asians. *Counter Terrorist Trends and Analysis*. Vol 7 Issue 4, pp 4 – 8. Retrieved from <https://www.rsis.edu.sg/wp-content/uploads/2015/06/CTTA-May-2015.PDF>

created an unprecedented situation where extremist teaching and material are readily available to the masses. ISIS excels at communicating its ideology via social media. We read of individuals who, in a matter of weeks or months, went from being ordinary citizens to becoming self-radicalised, and proceeding to carry out an attack. They act alone, under the radar of the authorities.

We see a shift in *modus operandi*, from targeting high signature, symbolic landmarks to hitting soft targets, like places of mass congregation, to inflict maximum casualties. We observe with horror how regular, easily accessible items like kitchen knives or cars have become part of the terrorists' arsenal. Much like the new breed of attackers who wield them, such items are not easily detected by security screening or intelligence gathering.

The approach of most governments in countering the threat of terrorism continues to be built on prevention and containment. It entails building up international networks, intelligence and enforcement capabilities to stop the threats before they happen, and to neutralise them quickly when they do happen. While these efforts remain crucial, they are no longer as effective in preventing the sort of attacks that we see today.

Increasingly, we have to recognise that the same typologies of attacks that took place in Westminster, Nice, Paris, Puchong, and Jakarta, can happen in Singapore.

What implications does this new reality carry in our fight against terror? Facing these threat scenarios requires a societal awareness that it is impossible for our security agencies to guarantee protection of our citizens at all times. There is a need to be upfront about our limitations and inability to deter all attacks. To stand up firmly and squarely against the threat

we face today, it has to be, and has become, a national imperative to enlist the support of all members of our community, to work alongside our security agencies to keep Singapore safe.

What Are the Changes Needed in Our Approach?

How then do we ensure that the community at large is prepared for the inevitable attack that slips through our robust security apparatus?

We first have to acknowledge that a mindset change among our community is needed. The Home Team has been able to keep Singapore safe and secure for many years, resulting in Singaporeans having a deep level of trust and confidence in the Home Team's abilities, arguably to the point of complacency. For instance, the 2015 National Security Awareness Survey found that residents were largely reliant on the Government to handle crises, if they arise. The longer that the Home Team is successful in keeping terrorist attacks at bay during this time of heightened threat, the further our people will remain complacent thinking that an attack will never happen here. We ironically have become the victims of our own success.

Moreover, when we look at communities elsewhere that have shown resilience in the face of terror, we observe that many have been challenged by previous crises. Bouncing back from such attacks have become an almost instinctive reflex in these communities. In contrast, Singapore has enjoyed prolonged peace, safety and security; we have not had similar crises to test and build our national resolve to bounce back.

In light of this, can we confidently say that Singapore will be able to effectively respond to and rebound from a terror attack when it occurs?

SGSecure – A Community-Oriented Solution

We cannot leave this question to chance. In the absence of a recent attack or crisis as a rallying point, we have to do everything in our power to prepare our people for an attack.

SGSecure is our way of galvanising a community response to terror. It is our national movement to sensitise, train, and mobilise our community to play a part to prevent and deal with a terrorist attack. It is how the whole of Singapore can come together in response to the terror threat, and safeguard our way of life. SGSecure focuses on three aspects in the fight against terror:

- **Vigilance:** Staying Alert to ever-present security threats
- **Cohesion:** Staying United during peacetime and in crisis
- **Resilience:** Staying Strong, to bounce back quickly after an attack

SGSecure builds on the decade-long cohesion efforts of the Community Engagement Programme (CEP), which was focused on the Cohesion aspect by building racial and religious harmony and a strong social fabric that aimed to help Singapore stay united in times of crisis. While it retains Cohesion as a key pillar, the SGSecure movement goes much further beyond CEP, to cover the Vigilance and Resilience aspects.

First and foremost, SGSecure seeks to jolt people out of complacency, and sensitise the community to the fact that an attack is imminent and that we need to be on our toes and stay alert. Through the SGSecure House Visits and an extensive publicity effort, we seek to create awareness and gain mindshare of the reality of

the terror threat. We have also developed the SGSecure app, which is used to alert residents to local incidents (i.e., a terror incident or a civil emergency) as well as attacks happening elsewhere in the world. Members of public can also report suspicious sightings to the authorities via the app.

Having captured our people's attention, SGSecure seeks to train and equip them with the necessary knowledge, skills and resources to respond at the immediate onset of an attack. One famous image from the Westminster attack was that of UK Foreign Minister Tobias Ellwood performing Cardiopulmonary Resuscitation (CPR) on an injured police officer. While the officer ultimately succumbed to his injuries, Mr Ellwood's actions had given the officer the best hope of survival. When an attack occurs, how affected persons respond in the first few minutes before emergency responders arrive is crucial. Our chances of survival are improved by knowing how to quickly get ourselves out of harm's way and how to help those who are wounded once we are safe. This is a key message that connects with Singaporeans and helps them realise the importance of picking up useful advisories and skills such as 'Run, Hide, Tell', Improvised First Aid Skills, and CPR-AED.

Finally, it is equally crucial that our community be psychologically prepared to deal with the 'day after' an attack, to stay united and go about life as per normal. For example, after the Westminster attack, Prime Minister Theresa May rallied the British people to do two things. Firstly, to unite and move forward together, and not allow terror to drive them apart. Secondly, to go about their lives as per normal the day after. The British people were able to do both. They pulled together, refused to be cowed, and went back to normal life almost immediately. Even the legendary British humour became a sustaining force against the

terrorists. While terror attacks continue to plague the UK, their way of life has not been disrupted.

The same outcome can only happen in Singapore if we take the effort to prepare our people today. SGSecure seeks to mobilise Singaporeans to come forward, and commit themselves to building and strengthening our spirit of unity and resilience that will enable us to decisively respond to and recover from a terrorist attack.

How is SGSecure Being Implemented on the Ground?

We have been systematically reaching out to individuals and organisations in Singapore to come on-board this national movement.

For individuals, the emphasis is on being sensitised to the threat, staying vigilant, knowing what to do when an attack happens, and building strong community bonds in peacetime. For organisations, our programmes further extend to supporting them in preparing contingency plans, running exercises to validate these plans, and ensuring that the organisation is ready to go back to normal soonest after an attack occurs.

To achieve these outcomes, the SGSecure Programme Office (SSPO) has partnered with other Government agencies to develop and roll out programmes in various domains. We started out in 2016 with a focus on programmes in the neighbourhoods and schools to reach and sensitise broad segments of the population.

Some good progress has already been made. As of 24 Sep 2017, a year after SGSecure was officially launched, we have reached out to around 220,000 households through the SGSecure House Visits. We have engaged students in more than 160 secondary schools

through our SGSecure Mobile Exhibitions and School Talks. Almost 1 million devices have been equipped with the SGSecure App. Even as we continue these programmes, we are also deepening engagement in the workplaces, with religious and community organisations, the media, and our National Servicemen (NS-men).

More than just numbers, there is a general sense that the public is more sensitised to the reality of the terror threat. For instance, we have received many reports from members of public on suspicious behaviour via 999 calls as well as via the SGSecure app. Members of public are paying close attention to their surroundings, and are not hesitating to report potential threats to the authorities.

The public response to the precautionary closure and evacuation of Hougang and Woodleigh MRT stations in two separate incidents in April 2017 was illustrative and encouraging. They showed that most Singaporeans understood that these were potential security threats, and the inconvenience of the station closures was an acceptable price to pay for our overall security.

The Way Forward - Awareness to Preparedness

SGSecure is still in its nascent stages, and there is much more to do in the months and years ahead. We have to maintain the momentum that has been generated and continually adapt to the changing security landscape.

Our programmes have focused primarily on raising awareness and sensitising people to the terror threat. While such programmes remain crucial, mere head knowledge of the threat is not enough. More needs to be done to drive in-depth training of individuals in relevant emergency-related skills.

Another significant area of focus will be to introduce more programmes to enhance organisational preparedness. Singapore will need schools, workplaces, organisations, transportation, and other essential services to keep functioning as normal, in order to resume the usual rhythm of daily life after an attack. This requires us to support more organisations to review their contingency plans and security infrastructure, and consider whether these are sufficient in light of the current threat level and new *modus operandi* of terrorist attacks. It demands that organisations commit to running exercises to stress-test and validate these plans.

In this area, we have started to roll out some programmes to enhance organisational preparedness in the various domains. For example, our Crisis Response Exercises in the neighbourhoods, conducted in partnership with the People's Association and grassroots organisations, aim to build capabilities among community and grassroots leaders to manage communal tensions and shore up our cohesion in the aftermath of an attack. We have also worked with the Ministry of Manpower to roll out a SGSecure Guide for Workplaces, to provide practical steps for employers to strengthen workplace resilience.

Finally, we must continue to strengthen our social fabric to ensure that we will stay united in the wake of an attack. We are working with partners, for example the Ministry of Community, Culture and Youth (MCCY), to roll out community building programmes. The SGSecure Community Network programme, for example, strengthens partnerships with religious and community organisations to build greater mutual trust and understanding. Most importantly, we must continue to encourage our people to deepen bonds across communities, and strengthen ties and relationships in our neighbourhoods, schools and workplaces

to provide a strong foundation.

SGSecure Transformation of the Community – Be Prepared, Our Response Matters

Since its launch in September 2016, the initial phase of the SGSecure movement has served as an 'electric shock', to inject life and energy into the various domains, to engage individuals and organisations to sensitise them to the terror threat, create an impetus to prepare and be ready for an attack, and seed broader ownership of our response to terrorism.

This goal of seeding broad ownership of the counter-terrorism agenda is crucial. With SGSecure, the Government is acknowledging that even with its best efforts, it may not be able to stop an attack. This means that our people must step up and do their part to protect themselves and others. Members of our community must be dynamic and proactive, to be partners with the Government in this endeavour.

This is a transformation of the Government's typical approach to security. It requires the Government to accept a certain degree of fallibility, not for want of trying, but as a consequence of the nature of current terrorism trends. We should not be deterred by this acknowledgement and, in fact, should ride on this reality to create a greater sense of urgency and motivation among members of the community to do something positive and constructive. The outcome will be a multi-faceted and sustainable counter-terrorism response that is needed to face the threats of today and tomorrow.

We must be ready as a country when the time comes to face an attack. We must be prepared, for each of our responses matters.



About the Author

Tan Jin Rui Jerald, Superintendent of Police, was awarded the Singapore Police Force Overseas Scholarship in 2005. He graduated with a Master of Engineering Science from the University of Oxford, UK, and started active service in SPF in 2009. His previous postings include Commanding Officer, Hougang Neighbourhood Police Centre, and Head Operations and Training, Tanglin Police Division.

He is currently at the Ministry of Home Affairs, where he holds the position of Senior Assistant Director (Policy), SGSecure Programme Office, Community Partnership and Communications Group.

The Psychology Behind Singapore's Terrorist Rehabilitation Strategy & Best Practices In Countering Violent Extremism

By Counter-Terrorism Division
Internal Security Department

The term 'countering violent extremism' (CVE) has become popular in recent years, as both academics and practitioners alike recognise that there is a need for multi-faceted and multi-disciplinary approaches to deal with the threat of violent extremism (Atran 2004; Crelinstern, 2009). While there seems to be no unanimous agreement on the definition of CVE (Heydemann, 2012), the concept is typically understood as efforts at reducing the number of terrorism-related activities through non-coercive means (McCants & Watts, 2012).

In 2001 and 2002, when Singapore was faced with a terrorism threat from the Jemaah Islamiyah (JI), there was early recognition that security and enforcement methods alone would not be sufficient to address the threat holistically. Importantly, there was an appreciation of the need to counter the ideas that the terrorists propagate, if radical influences are to be prevented from taking root in the

psyche of local society. In this regard, two key components of Singapore's counter-terrorism approach were initiated, namely the rehabilitation of individual terrorists, and the community-wide counter ideology efforts.

Countering the Misuse of Religion

The terrorism threat to Singapore today is at its highest since the disruption of the plots by Al-Qaeda (AQ) and JI in late 2001/early 2002. While AQ and JI continue to be a threat today, the terrorism threat now emanates from a wider set of actors. One of these actors is the Islamic State in Iraq and Syria (ISIS) which poses the most serious threat at this time. Another set of actors are self-radicalised home-grown terrorists. While self-radicalisation is not a new phenomenon in Singapore – we detained our first self-radicalised individual in 2007 – the rise of ISIS and its adept use of social media has resulted in the swift increase

in the number radicalised through cyberspace. After the rise of ISIS in 2014, 19 self-radicalised individuals have been dealt with under the Internal Security Act (ISA) – 12 are under detention and seven have been placed under Restriction Orders (RO). This is in contrast to the eight year period between 2007 and 2014, when five Singaporeans were detained and six were issued ROs, because of their radicalisation.

Despite the evolution of the terrorism landscape in Singapore, there continues to be a commonality inherent in the terrorism threat – the misinterpretation and misuse of religious concepts to justify acts of violence and to influence people to support the terrorists' cause. Given this background, the over-arching focus of Singapore's counter-terrorism strategy has been and will continue to be focused on terrorist rehabilitation and to build the community's resilience against radical rhetoric. This article will provide a brief summary of Singapore's counter-ideology strategy and identify several best practices based on the Singapore experience.

The detained terrorists in Singapore undergo a holistic rehabilitation programme which consists of psychological rehabilitation (through engagement with psychologists on issues like their psychological reasoning, in order to establish their propensity for hatred and violence), religious rehabilitation (by volunteers from the Religious Rehabilitation Group (RRG) to educate the detainees on the proper teachings and interpretations of Islam and counter the radical ideology they had imbibed) and social rehabilitation (visits by family members and case officers, as well as access to a library and opportunities to pursue further education). On the other hand, the community-wide counter ideology efforts are focused on inoculating the community and enhancing its resilience to the influence of ter-

rorist ideology. There is an active involvement in outreach efforts by various groups and even individuals who seek to lend their voice to the counter-ideology efforts.

The Value of Therapeutic Jurisprudence in Terrorist Rehabilitation

For the purpose of this paper, a psycho-legal and resilience perspective will set the stage in outlining several best practices from Singapore's experience in CVE. Within the psycho-legal approach, a concept which has received attention in the academic literature is therapeutic jurisprudence (TJ), an area of law that emphasises the improvement of one's psychological well-being. TJ was developed in the 1990s as an interdisciplinary approach, consisting of legal, criminological and mental health fields (psychology, psychiatry) to acknowledge the role of law in inducing change and enhancing well-being (Wexler, 1996). One of the key assumptions of TJ is that the way a law is implemented and operates can have a positive, neutral or negative impact on a person's well-being (Birdgen, 2002). Thus, the notion of a non-human agent contributing to (positive) change that is implicit within TJ can be further expanded to include how other operating procedures within a legal framework (e.g., in a prison setting, and how trials are conducted) can also facilitate positive change.

Given this theoretical perspective, there is a need to acknowledge the importance of having effective legislation as part of any counter-terrorism strategy, that can facilitate swift and effective response to potential terrorist and/or radicalisation threats. In Singapore, the ISA has been instrumental in allowing the authorities to act early, quickly and decisively against threats to the safety and security of Singapore. For example, in April 2015, a youth (which we will call 'H') attracted security attention because he supported ISIS and its ideology

of violence, and wanted to join the terrorist group. Beyond this, 'H' was also prepared to carry out attacks in Singapore against key facilities and to assassinate government leaders if he was prevented from leaving Singapore. 'H' had been radicalised after viewing terrorist propaganda online. The ISA allows the Internal Security Department to intervene early to neutralise the threat posed by individuals such as 'H'.

A key feature of the ISA is preventive detention, which allows early intervention to neutralise the threats posed by potential terrorists and/or radicalisation threats. The ISA has robust checks and balances built-in. For example, unlike a court sentence which is fixed, the ISA allows individuals to be detained for a maximum period of two years at any given time. If subsequent preventive detention of these individuals is still warranted, it must be approved by the Minister of Home Affairs and the President of Singapore; otherwise they will be released. "H" and others detained under the ISA for terrorism-related activities, are placed on a rehabilitation programme to help wean them off the radical ideology which they had imbibed. From the TJ perspective, the provision within the ISA of not having a fixed term for the detention provides the detainees with an opportunity to take ownership of their rehabilitation. That is, their release is dependent on how receptive they are to rehabilitation. If they have done their best to change and are genuine about being rehabilitated, they can expect a shorter detention term. The provisions within ISA are thus consistent with the key element of TJ, where the law encourages the detainees to take ownership of the issues which led them down the path of radicalisation, and to take their rehabilitation endeavours seriously.

Singapore's ISA is a historical legacy from its colonial days, enacted long before concepts

like TJ were developed. Regular reviews of its procedures to give detainees legal protections, such as access to lawyers and the right to challenge the evidence used to justify their detention, along with the comprehensive system of rehabilitation and re-integration, have allowed the ISA to be used to not just neutralise terrorist threats but also to support therapeutic jurisprudence. Singapore's experience with preventive detention provides a best practice: countries in the process of reviewing their laws to deal with the threat of terrorism have an opportunity to consider how TJ can be incorporated into their laws in ways that will allow these laws to better regulate behaviours within society, including those related to terrorism.

The second best practice can be gleaned from how Singapore has used rules and operating procedures in prisons where terrorism offenders are held to induce change. Proponents of TJ have noted that rules and operating procedures can serve as catalysts to ensure that 'therapeutic effects of the law can be maximized and anti-therapeutic effects be minimized' (Birdgen, 2002). In Singapore, the rehabilitation strategy requires that detainees not be allowed to interact with other detainees. Grouping them with other detainees would give rise to negative group dynamics that might impede rehabilitation. The Singapore system places emphasis on the need for the individual to do more self-reflection and increase his receptivity to the messages from the various rehabilitation stakeholders, in order to counter the violent ideology they had previously been taught.

The detainees, upon their release, will have to further strengthen their resilience to radical influences as they re-integrate into society. The released detainees are typically put on a Restriction Order (a provision within ISA) and rehabilitation continues for them. This provides the context for the intersection of TJ

and the resilience perspective, to ensure that ex-detainees do not revert to their violent, radical past. One of the models used to elaborate on building resilience is that of the Linking Human Systems Community Resilience Model (LINC; Landau 2007). LINC begins with the assumption that individuals, families and communities have the necessary competencies to develop resilience against a negative event. This means that each of these different units or levels of society can be a resource for the other, in times of stress and adversity (Landau, 2007).

Building community resilience

A LINC perspective thus brings us to the third best practice based on Singapore's experience in CVE: there is a need for a rigorous post-release supervision programme to ensure that those released from detention do not re-engage in terrorism activity after their release. In Singapore, three main tenets of the post-release supervision programme are emphasised. First, a case officer will be assigned to the ex-detainee to: (i) ensure compliance to the RO; (ii) facilitate reintegration into society; and (iii) follow through with the rehabilitation programme. Second, the role of the family members in supporting the ex-detainee is also stressed, where the family can assist by providing a censoring environment to monitor and prevent the ex-detainee from reverting to his old ways.

To successfully re-integrate into society, it is also critically important for RO supervisees to be employable. To this end, the case officer will sometimes assist in obtaining employment for the ex-detainees if they have problems finding employment on their own. Such assistance also provides the case officer regular access to the employers to get updates on the progress made by the ex-detainees on their reintegration. Third, the ex-detainees continue to at-

tend religious counselling and weekly religious classes. These sessions allow the ex-detainees to clarify any remaining doubts and to gain an objective understanding of the religious concepts.

One ex-detainee described his re-integration experience thus:

Due to the support and help my family received (from ISD and Muslim welfare groups), I was able to re-integrate into the society fairly quickly. I was not treated like an outcast and my neighbours were friendly and polite to me. (Hussain, 2012).

The fact that this and other ex-detainees are largely able to re-integrate well shows the usefulness of adopting the LINC perspective in linking and harnessing the spirit and resources of the collective (case officer, family and employers) to bring about positive change at the individual (in this case, the ex-detainee) and societal level.

Lastly, in acknowledging that different levels of a society like families and communities possess the resources to enhance resilience (in this case, against radical influences), there is value in enhancing the community partnership programmes as a strategic and upstream approach in CVE. Families and communities (including various welfare and self-help groups) have a critical role in fostering an environment that does not sanction the spread of violent ideology in society, while providing support to those who have family members who fell prey to radical ideologies.

From the LINC perspective, (re-)deploying existing community resources in response to a problem in society is preferred to establishing seemingly artificial and specific support infrastructure. The final decision-making with regard to how resources are utilised is left to the community groups themselves (Landau,

2007). Given this context, the setting up of the Inter-Agency Aftercare Group (ACG), which comprises community groups like Association of Muslim Professionals, Yayasan Mendaki, Taman Bacaan and Khadijah Mosque, to assist the families of detainees, embodies the key tenets of LINC, where existing community resources are re-deployed to address a specific problem (i.e. the practical support needed by families of detainees). The ACG also facilitates the re-integration of ex-detainees; in one interview, an ex-detainee said he felt 'very happy and looked forward to (my) studies' after he sought financial assistance from Yayasan Mendaki to help him complete his tertiary education (Hussain and Kader, 2015).

The ACG, in relying on community networks, has also since moved from just providing practical support to (ex)detainees and their families, to organising youth forums to increase awareness of the terrorism threat. The expansion of the role of ACG is illustrative of the LINC perspective in that communities do indeed possess the resources to address issues in society, including the threat posed by terrorism.

On another level, the role of the RRG in Singapore's counter-terrorism approach underscores the importance of having a close partnership between the government and community, working in concert to counter the terrorism threat. The RRG involvement also expounds on the notion that the appropriate resources which are sometimes needed to deal with the threat (in this case, appropriate religious understanding and interpretations) are indeed available in the community, waiting to be harnessed and deployed to address the problem. This again underscores the fundamental tenet of LINC: that communities possess the relevant resources to overcome problems, and thus engaging communities on a range of issues, including terrorism, should

be pursued, valued and enhanced.

Conclusion

In conclusion, terrorism is a persistent threat and Singapore will remain a prime target for terrorists. The impact of an attack in Singapore goes beyond the physical harm to lives and property, because it will also create suspicion, tension and even strife among the various racial and religious groups in Singapore. In Singapore, the dual approach of terrorist rehabilitation and community-wide counter ideology efforts has been instrumental in our fight against terrorism. By providing a psychological perspective to Singapore's experience in dealing with the terrorism threat, it is hoped that others can appreciate some of the considerations and underlying principles driving the two approaches, and how they have worked well thus far. The role of laws and the importance of communities working together and harnessing each other's resources will go a long way towards ensuring that Singapore remains safe and secure.

About the Author

The article was contributed by ISD's Counter-Terrorism Operations Division which has a team of psychologists involved in the rehabilitation programme for detainees of violent extremism.

References

- Atran, Scott. (2004). Mishandling suicide terrorism. *The Washington Quarterly* 27, 67-90.
- Birdgen, Astrid. (2002). Therapeutic jurisprudence and "good lives": A rehabilitation framework for corrections. *Australian Psychologist* 37, 180-186.
- Crelinstern, Ronald. (2009). *Counterterrorism*. Cambridge: Polity Press.
- Heydemann, Steven. (2012). Countering violent extremism as a field of practice. *United States Institute of Peace Insights* 1, 9-11.
- Hassan, Muhammad Haniff., & Mostarom, Tuty Raihanah. (2011). A decade of combating radical ideology: *Learning from the Singapore Experience*. Singapore: S. Rajaratnam School of International Studies.
- Hussain, Zakir. (2012, January 7). What Jemaah Islamiyah did was wrong, convicted terrorist says. *The Straits Times*. Retrieved from <http://jakartaglobe.id/archive/what-jemaah-islamiyah-did-was-wrong-convicted-terrorist-says/>
- Hussain, Zakir., & Kader, Abdul Halim. (2015). Interagency aftercare group: *Fostering social reintegration and building community resilience*. Singapore: Singapore Malay Youth Library Association.
- Landau, Judith. (2007). Enhancing resilience: Families and communities as agents for change. *Family Process* 46, 351-365
- McCants, William & Watts, Clint. (2012, December 10). U.S. Strategy for Countering Violent Extremism: An Assessment. Foreign Policy Research Institute. Retrieved from <http://www.fpri.org/article/2012/12/u-s-strategy-for-countering-violent-extremism-an-assessment/>
- Ministry of Home Affairs. (2002). *Internal Security Act*. Retrieved from https://www.mha.gov.sg/Newsroom/speeches/Documents/ISA_Booklet-English.pdf
- Singh, Bilveer. (2016). Revising Indonesia's anti-terrorism laws. *RSIS Commentary* 57. Retrieved from <https://www.rsis.edu.sg/wp-content/uploads/2016/03/CO16057.pdf>
- Wexler, David B. (1996). Therapeutic jurisprudence and changing conceptions of legal scholarship. In D.B. Wexler & B.J. Winnick (Eds.), *The law in a therapeutic key: Developments in therapeutic jurisprudence*. Carolina: Carolina University Press, 645-668.

Comparing ISIS Foreign Fighters versus Sympathisers: Insights from their Twitter Postings

By Neo Loo Seng and Dr. Majeed Khader
Home Team Behavioural Sciences Centre
Ministry of Home Affairs, Singapore

Dr. Joyce S Pang
Nanyang Technological University, Singapore

Abstract

This study will attempt to map a set of personality and psycho-social factors to the social media postings of two groups of individuals who were influenced by propaganda material about or from the Islamic State in Iraq and Syria (ISIS). The aim of this study is to see if – and how – the social media postings of the individual actor can be used to distinguish foreign fighters (i.e., individuals who travelled to join ISIS) from sympathisers (i.e., individuals who did not travel to join ISIS). 622 tweets posted by a sample of three foreign fighters and three sympathisers were mapped against 12 factors. Mean interrater reliability was .81, and ranged from good to excellent across all variables. One significant difference (i.e., readiness to use violence) was found between the two groups and the finding has opened new direction for further research, with the goal

of providing empirical support for the online threat assessments of violent extremists.

Which online violent extremist goes on to fight?

In recent years, the notion of online violent extremism has gained traction. Violent extremists of all stripes have extensively used the Internet to propagate their message and gain new followers and sympathisers (Conway, 2007; Egan et al., 2016; Gill, 2015; Weimann, 2004). The unfolding of the 2013 attack on the Westgate Mall in Nairobi, Kenya was ‘live tweeted’ by Al-Shabaab through its twitter account to inform followers of the developments as well as to draw attention to the group’s cause. The internet has also afforded greater opportunities for violent extremists to radicalise and mobilise others into action (Gill

et al., 2017). In fact, there is an increase in the number of individuals who have been radicalised via the Internet. Consistent with the ideas and ideologies they consumed on the Internet, some of these individuals then transited offline to carry out real world violence against targets (Edwards & Gribbon, 2013; Neo, Dillon, & Khader, 2016; Neumann, 2012). This therefore warrants special emphasis to understand violent extremists' online behaviours.

The recent rise of the Islamic State in Iraq and Syria (ISIS) has revolutionised the way violent extremists used the Internet, and in particular social media platforms. As Klausen (2015, p. 4) argues: 'Social media has changed the dynamic fundamentally. It has eliminated the terrorists' dependency on mainstream media, reversing the relationship by making mainstream media dependent on the jihadist-run social media.' Through the use of its social media platforms, ISIS has inspired an unprecedented surge of individuals to leave their homeland and travel to the Middle East in order to join the group (Carter, Maher, & Neumann, 2014; Mans & Tuitel, 2016; Dawson, Amarasingam, & Bain, 2016). Credible estimates now suggest that more than 30,000 fighters have travelled to Syria since 2012, originating from more than 90 different countries (The Soufan Group, 2015).

However, in this online milieu where violent extremists operate, it is important to note that while there are many members of the online violent extremist community, very few become violent extremists or law-breakers in the real world. The 'loudest' online members (i.e., those engaged in the most vigorous and aggressive forms of speech) may not, in fact, be the ones most likely to engage in violence, while the most passive members are not automatically the most peaceful. It is not possible, in other words, to draw a straight line between online 'noise' and offline action.

In the context of ISIS, while its foreign fighters have become a dominant security concern, there is a need to be cognisant of the 'stay home supporters' (i.e., sympathisers) who have not been mobilised despite being part of the same online violent extremist community from which the foreign fighters were recruited (Vidino & Hughes, 2015). There is therefore a need to examine how researchers and analysts can harness such online information to better assess the threat posed by those who espouse violent extremism online.

Insights from communication literature suggest that personal attributes can be gleaned from studying the social media footprint of targeted individuals. For example, Alam, Stepanov, and Riccardi (2013, p. 6) argue that 'there is a strong correlation between users' personality and the way they behave on online social network'. Furthermore, social media profiles are found to be reflective of the users' actual personality, contrary to the assumption that people tend to present only highly favourable or desirable news or information about themselves online (Back et al., 2010).

Hence, it is possible to derive insights about an individual's personality based on their social media activity. Patterns of their worldviews, preferences, and expressions can be 'read' and interpreted to identify their personality traits. However, it is not just personality traits that reveal themselves online. A study by Kosinskia, Stillwell, and Graepel (2013) has shown that social media analysis can also offer a window into a broad range of characteristics, including propensity for recreational drug use, status of parents' marriage, preference for certain sports and teams, and, of course, political and religious views. The latter are particularly important in the context of understanding online support for violent extremism. As Pressman and Ivan (2016, p. 404) suggest, 'data on the views, beliefs, attitudes, grievances, intentions

and ideology of identifiable individuals can be captured from the internet'. The authors further argue that social media platforms provide important opportunities for law enforcement and intelligence agencies to gain knowledge of violent extremists.

Thus, this paper aims to ascertain if there are any personality and psycho-social factors that distinguish sympathisers from those planning to break the law or engage in real world violence (i.e., foreign fighters). To answer this question, relevant factors based on literature review that outline patterns of violent extremists' online activities (see Neo, Dillon, & Khader, 2016; Neo, Dillon, & Tan, 2016) were mapped against ISIS foreign fighters and ISIS sympathisers.

Methodology

Research design

Given that these foreign fighters and sympathisers have published remarkable amounts of highly personal and detailed information on their social media accounts, this allows the authors the opportunity to download their social media postings for comparison. For the purpose of this study, the social media output (i.e., tweets from Twitter) of the foreign fighters and sympathisers were mapped to the factors as highlighted in Table 1. These factors were derived from a literature review of extant violent extremism risk assessment tools such as the Extremist Risk Guidance 22+ (Lloyd & Dean, 2015), the Identifying Vulnerable People [IVP] guidance (Egan et al., 2016), the Terrorist Radicalisation Assessment Protocol [TRAP-18] (Meloy, Roshdi, Glaz-Ocik, & Hoffmann, 2015), the Violent Extremist

Risk Assessment [VERA-2] protocol (Pressman & Flockton, 2012), and the Cyber-VERA (Pressman & Ivan, 2016).

Sampling procedure

As this study aims to identify the factors that may distinguish individuals who have moved beyond the role of a sympathiser to that of a foreign fighter, the Twitter accounts of ISIS fighters (i.e., supporters of ISIS who have travelled to Syria and engaged in real world violence) and ISIS sympathisers (i.e., supporters of ISIS who neither travelled to Syria, nor engaged in real world violence) were selected for comparison.

Criteria for sample

The decision to include the Twitter accounts of potential foreign fighters and sympathisers in the current study was based on the following criteria:

The account must be affiliated with ISIS, based on the content and context of the media postings sent from these accounts (see figure 1);



Figure 1. Account affiliated with ISIS

Table 1. Personality, Psychosocial, and Protector Factors of Online Violent Extremism

Domain	Factor	Indicator	
Personality	Perceived grievances (PG)	PG1	Publicise the injustices targeted at one's own community, faith, or belief
		PG2	Demonstrate a preoccupation with a certain group(s) of concern believed responsible for the injustice
		PG3	Express frustration with the injustice targeted at one's own community, faith, or belief
		PG4	Express a strong sense of hatred towards a certain group(s) of concern believed responsible for the injustice
		PG5	Openly challenge certain group(s) of concern about the injustice
	Intolerance towards multi-religious, multi-racial living (I)	I1	Force friends, colleagues or family to distance themselves from certain group(s) or community
		I2	Dehumanise group(s) of concern who hold different viewpoints/ beliefs system
		I3	Dissatisfaction with local cultures, practices, values, and governance
		I4	Anti-integration messaging – exclusivity of one's own community, faith, or belief
	Knowledge and skill to commit violent extremist offences (K)	K1	Demonstrate an interest in learning combat skills
		K2	Showcase interest in the use of weapons and explosives
		K3	Have information on explosives-bomb making
	Redemption and the pursuit for significance (S)	S1	Desire to partake in humanitarian activities in countries associated with violent extremism opportunities
		S2	Desire to repent by migrating to countries associated with violent extremism opportunities
		S3	Express feelings of contempt for own prior practices
		S4	Intention to search for opportunity to do something meaningful
	Susceptible to influence (SI)	SI1	Desire to explore different ideologies and beliefs – inconsistent identity
	Readiness to use violence (R)	R1	Voice strong support for the use of violence towards a certain group(s) of concern as a viable solution
		R2	Incite friends, colleagues or family to join the violent extremist cause to defend his/her faith, religion or belief
		R3	Express willingness to die for cause, and achieve martyrdom
		R4	Demonstrate a preoccupation with an individual from group(s) of concern as a potential target
		R5	Display himself/herself as a protector/hero of his/her fellow believers of the same faith, religion or belief
		R6	Perceive an urgency to act and that non-violent alternatives are ineffective solutions
		R7	Indicate his/her intention to travel and participate in overseas conflict

Table 1. Personality, Psychosocial, and Protector Factors of Online Violent Extremism

Domain	Factor	Indicator	
Psychosocial	Commitment to violent extremist groups (C)	C1	Quotations from / associations with personalities known for their violent extremist views
		C2	Identify with symbols of known violent extremist groups on one's online profile
		C3	Display his/her public allegiance to violent extremist groups
		C4	Praise and defend violent extremist groups
	Online relationship building with like-minded individual (OR)	OR1	Attempt to reach out to violent extremists
		OR2	Develop and disseminate violent extremist content
		OR3	Attempt to set up physical meeting with violent extremists
	Involvement in online community (OC)	OC1	Possess violent extremist documents, music, videos etc. on computer or mobile devices
		OC2	Host web-links to other online platforms that contain violent extremist content
		OC3	Subscribe to sources that propagate violent extremist ideologies, news or in-group favouritism
		OC4	A sudden increase in the user's activity
	Negative social support (N)	N1	Presence of supportive family members and friends that encourage extremist offending
	Protective	Individual-centric protective elements (IP)	IP1
IP2			Demonstrate willingness to engage in discussions of ideology and the use of violence
IP3			Disillusioned with using violence to solve problems
IP4			Demonstrate an appreciation for diversity
Online environment-centric protective factors (OP)		OP1	Inability to obtain access to online community
		OP2	Recognise and fear detection by law enforcement and social media companies

- The identified accounts belong to individuals and are not accounts belonging to a group or a communal account run by several users;
- The accounts were active during the period of 2013 to 2015¹ – this period was the time where most of the ISIS foreign fighters made the travel to Syria and Iraq to join ISIS; and
- The selected Twitter accounts originated from the United Kingdom.

In order to ensure that the account was authentic and belonged to a foreign fighter, there was a need to look for evidence such as pictures of them in combat, reference to/from other foreign fighters, description of battles, description of migration, descriptions of life in Syria and Iraq which tally with other accounts of life there. In contrast, sympathisers were identified based on the evidence of support for ISIS in their media postings, such as viewing ISIS' activities in a sympathetic light and being able to express a high level of knowledge about ISIS' history and developments.

*Identification of sample*²

The authors used their own Twitter accounts to identify potential foreign fighters and sympathisers from the UK. Many of the leads came from news stories, blogs, reports released by law enforcement agencies, academic literature on ISIS, think tanks, discussions with academics and practitioners, and recommendation al-

gorithms by Twitter.

In total, three foreign fighters and three sympathisers from the United Kingdom were identified for the purpose of this exploratory study. Even though there are only three subjects per group, the richness of the qualitative data permits the authors to make comparisons between the two groups. These are also individuals whose case information was available in the public domain via Twitter. The sample of foreign fighters was picked because of the availability of rich online histories prior to their departure to join ISIS. The sample of sympathisers was obtained by identifying individuals with rich online histories, and had not made the trip to travel to Syria to fight for ISIS.

To ensure that a standardised comparison of content between the two groups can be performed, two additional guidelines were implemented. Firstly, the authors chose Twitter accounts of foreign fighters and sympathisers that approximated 100 tweets³ each. For the fighters, these were tweets taken from the time they set up the accounts until they made the travel. For the sympathisers, these were tweets taken from the time they set up the accounts until the accounts became inactive. Thus, this ensures that a similar number of tweets from each group was available for analysis. Secondly, the geographical location of both groups was kept constant as they were all residing within the United Kingdom when the tweets were created.

¹ There is no uniform collection from one ISIS supporter to the next. Some individuals may have more than two years' worth of Twitter activity preserved, whilst others have only a few months. In addition, many of the time periods for different ISIS supporters do not always overlap.

² Please contact the authors if you are interested in the names of the foreign fighters and sympathisers used in this study.

³ The selected accounts tweeted in the range of 70 to 130 tweets (plus or minus 30 tweets from the average 100 tweets).

Data coding procedure

Data coding

A codebook⁴ was developed based on the above-mentioned 42 indicators to guide and inform the coders about what to look out for. The coders were instructed to look at the overall context of the tweet (e.g., matching pictures with accompanying text and emoticons) to best decipher the attitudes, feelings, and opinions of the user. See for example, figure 2.



Figure 2. Identifying a tweet of concern based on the overall context of the tweet

For example, if a tweet quoted this verse of the Quran – ‘And I did not create the jinn and mankind except to worship me’ (51:56) – it would not be coded as a marker of violent extremist belief. However, if the same verse appeared in a tweet alongside a picture of a fighter, or suicide bomber, it could legitimately be taken as inferring jihad as a religious obligation.

All coding for the indicators was binary (present or absent), with a notation if there was insufficient information. Coders also recorded the number of instances an indicator was mentioned. This is particularly important because it allows the authors to obtain an objective estimate of the prevalence of the 42 indicators in the sample’s social media output.

Interrater reliability

Two independent coders were asked to code the Twitter accounts of the three foreign fighters and three sympathisers using the codebook after receiving instructions and practice in us-

ing it. Coders were blind to the status of the account holders (i.e., fighters or sympathisers). To measure the agreement between the two coders, Cohen’s kappa – which is a more robust measure than simple percent agreement calculation – was computed (Landis & Koch, 1977). All kappa values ranged from good to excellent [.78 to .86], and all were significant at $p < .001$; the mean kappa was .81. In other words, the coders exhibited a high level of agreement in terms of their coding.

Results

To examine the relationship between the factors and the social media postings of the foreign fighters and sympathisers, the presence or absence of each factor and its associated indicators was used for analysis. Table 2 lists each factor and its associated indicators, and how they were coded. Indicators that appeared in more than 50 percent (i.e., 2 out of 3 individuals) of the two subsamples were highlighted in orange. Factors that may distinguish fighters from sympathisers were highlighted in purple.

⁴ Please contact the authors if you would like to find out more about the codebook. The coders were research analysts who had at least one year of research experience on the topic of online radicalisation and violent extremism.

Table 2. Presence of Factors for Foreign Fighters and Sympathisers

Factor	Indicator	% Present in overall sample	% Present in Fighters	% Present in Sympathisers
Perceived grievances (PG)	PG1	100 (6)	100 (3)	100 (3)
	PG2	83 (5)	66 (2)	100 (3)
	PG3	66 (4)	33 (1)	100 (3)
	PG4	100 (6)	100 (3)	100 (3)
	PG5	66 (4)	66 (2)	66 (2)
Intolerance towards multi-religious, multi-racial living (I)	I1	50 (3)	33 (1)	66 (2)
	I2	33 (2)	33 (1)	33 (1)
	I3	100 (6)	100 (3)	100 (3)
	I4	100 (6)	100 (3)	100 (3)
Knowledge and skill to commit violent extremist offences (K)	K1	16 (1)	0 (0)	33 (1)
	K2	50 (3)	100 (3)	0 (0)
	K3	0 (0)	0 (0)	0 (0)
Redemption and the pursuit for significance (S)	S1	0 (0)	0 (0)	0 (0)
	S2	33 (2)	66 (2)	0 (0)
	S3	16 (1)	33 (1)	0 (0)
	S4	33 (2)	66 (2)	0 (0)
Susceptible to influence (SI)	SI1	0 (0)	0 (0)	0 (0)
Readiness to use violence (R)	R1	66 (4)	100 (3)	33 (1)
	R2	66 (4)	100 (3)	33 (1)
	R3	50 (3)	100 (3)	0 (0)
	R4	16 (1)	33 (1)	0 (0)
	R5	33 (2)	66 (2)	0 (0)
	R6	16 (1)	0 (0)	33 (1)
	R7	16 (1)	0 (0)	33 (1)
Commitment to violent extremist groups (C)	C1	83 (5)	66 (2)	100 (3)
	C2	50 (3)	33 (1)	66 (2)
	C3	33 (2)	66 (2)	0 (0)
	C4	83 (5)	66 (2)	100 (3)
Online relationship building with like-minded individual (OR)	OR1	66 (4)	100 (3)	33 (1)
	OR2	0 (0)	0 (0)	0 (0)
	OR3	16 (1)	33 (1)	0 (0)
Involvement in online community (OC)	OC1	33 (2)	0 (0)	66 (2)
	OC2	33 (2)	33 (1)	33 (1)
	OC3	66 (4)	100 (3)	33 (1)
	OC4	0 (0)	0 (0)	0 (0)
Negative social support (N)	N1	0 (0)	0 (0)	0 (0)
Individual-centric protective elements (IP)	IP1	0 (0)	0 (0)	0 (0)
	IP2	33 (2)	0 (0)	66 (2)
	IP3	0 (0)	0 (0)	0 (0)
	IP4	16 (1)	0 (0)	33 (1)
Online environment-centric protective elements (OP)	OP1	0 (0)	0 (0)	0 (0)
	OP2	0 (0)	0 (0)	0 (0)

Factors present in the majority of the foreign fighter subsample

18 indicators appeared in more than 50 percent of the foreign fighter subsample. These 18 indicators were from the following eight factors: perceived grievances (PG); intolerance towards multi-religious, multi-racial living (I); knowledge and skill to commit violent extremist offences (K); redemption and the pursuit for significance (S); readiness to use violence (R); commitment to violent extremist groups (C); online relationship building with like-minded individual (OR); and involvement in online community (OC).

Perceived grievances

For this factor, four out of five indicators appeared in more than 50 percent of this subsample: PG1 – 100 percent; PG2 – 66 percent; PG4 – 100 percent; PG5 – 66 percent. For example, the foreign fighters would:

- Publicise the injustices targeted at one's own community, faith, or belief (PG1): 'Wallahi, very sad seeing women cry after the explosion. Children were injured, Allahul must'aan' [sic].
- Demonstrate a strong preoccupation with groups that they deemed to be responsible for the injustice faced by Muslim (PG2): 'Abu_ilyaas91 akhi I can't give his info out as we know these kuffars ⁵ would add 638 lies' [sic].
- Exhibit a strong sense of hatred towards the groups responsible for the injustice (PG4): '@Panty_Python @ProxetSC2 @AbuAbdullah_

RT Yep we cut heads, it's been 90 years we got bullied now its time to turn the table' [sic].

- Openly challenge those viewed as responsible for the injustice (PG5): 'Do these kuffars think by killing Abu Bakr Al Baghdadi,⁶ they would stop Jihad?' [sic].

Intolerance towards multi-religious, multi-racial living

For this factor, two out of four indicators appeared in more than 50 percent of this subsample: I3 – 100 percent; I4 – 100 percent. For example, the foreign fighters would:

- Be dissatisfied with local cultures, practices, values, and governance (I3): 'Picture of a family begging in the street; Post: This is the situation of the ummah,⁷ while the mujahideens bring honour to Islam our Muslim people abandon them' [sic].
- Espouse anti-integration messaging – exclusivity of one's own community, faith, or belief (I4): 'I found a bible in my workplace by some next man who probs tryna give some shirky dawah.. Shall I burn it? He might of left it here tho?' [sic].

Knowledge and skill to commit violent extremist offences

For this factor, one out of three indicators appeared in more than 50 percent of this subsample: K2 – 100 percent. For example, the foreign fighters would:

⁵ Kuffar refers to a non-believer or someone who does not accept the divinity of Allah.

⁶ Abu Bakr al-Baghdadi is the leader of ISIS.

⁷ Ummah is an Arabic word meaning community.

- Showcase interest in the use of weapons and explosives (K2): ‘Picture of Ali Kalantar⁸ firing a weapon; Post: {And fight them until there’s no fitnah⁹ and (until) the religion, all of it, is for Allah...} 8:39’ [sic].

Redemption and the pursuit for significance

For this factor, two out of four indicators appeared in more than 50 percent of this subsample: S2 – 66 percent; S4 – 66 percent. For example, the foreign fighters would:

Exhibit the desire to repent by migrating to countries associated with violent extremism opportunities (S2): ‘2 married brothers went off for dogma. One of them didnt even tell his wife back home (not in sham). Wow these brothers know priorities!!’ [sic].

Showcase intention to search for opportunity to do something meaningful (S4): ‘If anyone wants to support a good cause... kik¹⁰ me and we can deal with it inshallah’ [sic].

Readiness to use violence

For this factor, four out of seven indicators appeared in more than 50 percent of this subsample: R1 – 100 percent; R2 – 100 percent; R3 – 100 percent; R5 – 66 percent. For example, the foreign fighters would:

- Voice strong support for the use of violence as a viable solution (R1): ‘Executed many prisoners yesterday, sold their deen for \$70 which they didn’t even get. #IS #Khilafa’ [sic].

- Incite friends, colleagues or family to join the violent extremist cause (R2): ‘Did Allah not provide for your family whilst you were in the womb? You do not control rizq, allah does so come here .. Allah wont let u down’ [sic].

- Express willingness to die for cause, and achieve martyrdom (R3): ‘40 brothers from my old khatiba gave bay’ah¹¹ to death, cut their own exit route, entered enemy ranks of 3000. Victory soon. #Iraq #IS’ [sic].

- Display himself as a protector of his fellow Muslim brother (R5): ‘Look how a few men that submit to their Lord and seek to meet Him are humiliating the armies of the world. #IS’ [sic].

Commitment to violent extremist groups

For this factor, three out of four indicators appeared in more than 50 percent of this subsample: C1 – 66 percent; C3 – 66 percent; C4 – 66 percent. For example, the foreign fighters would:

- Display associations with personalities known for their violent extremist views (C1):

⁸ Ali Kalantar was a 19-year-old British citizen who travelled to Syria to join ISIS as a foreign fighter. He has since been killed in combat.

⁹ This refers to unrest or rebellion, especially against a rightful ruler.

¹⁰ Kik is a freeware instant messaging mobile application.

¹¹ This refers to an oath of allegiance to a leader.

‘ahmadmusajibril¹² I love you for the sake of Allah. You know how to remove doubt may Allah reward you’ [sic].

- Display his/her public allegiance to violent extremist groups (C₃): ‘We are no longer The islamic state of iraq and sham. We are only the ‘ISLAMIC STATE’. It’s official khilafa is restored!’ [sic].
- Praise and defend violent extremist groups (C₄): ‘Theres no brotherhood like tht in Jihad. Make dua 4 the ikhwa¹³ here, wallahi thy look afta u. May Allah unite us in Jannah’ [sic].

Online relationship building with like-minded individual

For this factor, one out of three indicators appeared in more than 50 percent of this subsample: OR₁ – 100 percent. For example, the foreign fighters would:

- Attempt to reach out to violent extremists (OR₁): ‘@IbnShaheed wallah I wanted to tell u guys but had to keep it low. U gt my kik, if I hav net there...’ [sic].

Involvement in online community

For this factor, one out of four indicators appeared in more than 50 percent of this subsample: OC₃ – 100 percent. For example, the fighters would:

- Subscribe to sources that propagate violent extremist ideologies, news or in-group favoritism (OC₃): ‘RT @truthsMaster: #BREAKING US AIR FORCE JETS BOMBED HOUSES

OF CIVILIANS IN DOMIEZ, SINJAR INSTEAD OF ISLAMIC STATE ARTILLERY POSITIONS!’ [sic].

Factors present in the majority of the sympathiser subsample

14 indicators from five of the factors appeared in more than 50 percent of the sympathiser subsample: perceived grievances (PG); intolerance towards multi-religious, multi-racial living (I); commitment to violent extremist groups (C); involvement in online community (OC); and individual-centric protective elements (IP).

Perceived grievances

For this factor, all the five indicators appeared in more than 50 percent of this subsample: PG₁ – 100 percent; PG₂ – 100 percent; PG₃ – 100 percent; PG₄ – 100 percent; PG₅ – 66 percent. For example, the sympathisers would:

- Publicise the injustices targeted at one’s own community, faith, or belief (PG₁): ‘Shia militants burning #Adhamiyah a Sunni neighborhood in #Baghdad.. #Iraq #ISIS <http://t.co/HibKd7wJXq>’ [sic].
- Demonstrate a strong preoccupation with groups that they deemed to be responsible for the injustice faced by Muslim (PG₂): ‘What treaty?? Didn’t America invade our lands rape our women torture us and kill our children, what treaty are u talking about’ [sic].
- Express frustration with the injustice targeted at the Muslim community (PG₃): ‘Your

¹² Ahmad Musa Jibril is a Palestinian-American Islamic radical preacher.

¹³ Jihadists like to refer to each other as ikhwan or brother.

duty is to convey the message. Not to become a welcome mat for the kuffar in hopes that they become muslim. It wont work' [sic].

- Exhibit a strong sense of hatred towards the groups deemed responsible for the injustice (PG4): 'When they take over Turkey and have a strong airforce, then CAR we are coming for you. Burma, we are coming for you' [sic].
- Openly challenge those viewed as responsible for the injustice (PG5): 'Why dont the kuffar just let us leave?! You dont want us there, yet you dont want us to leave either! Hypocrites!' [sic].

Intolerance towards multi-religious, multi-racial living

For this factor, three out of four indicators appeared in more than 50 percent of this subsample: I1 – 66 percent; I3 – 100 percent; I4 – 100 percent. For example, the sympathisers would:

- Force friends, colleagues or family to distance themselves from the West (I1): 'Do not support the trinity of evil (Israel, America, Peshmerga) you will end up in a blazing fire' [sic].
- Be dissatisfied with local cultures, practices, values, and governance (I3): 'Rafidhi Iraqi utes are so wasted, all they do smoke is Shisha and talk about girls, They swarm my area like mad' [sic].
- Espouse anti-integration messaging – exclusivity of one's own community, faith, or belief

(I4): 'IS destroyed Palmrya's prison because it was a symbol of oppression and humiliation to Muslims, We are not kuffar to make a memorial of it' [sic].

Commitment to violent extremist groups

For this factor, three out of four indicators appeared in more than 50 percent of this subsample: C1 – 100 percent; C2 – 66 percent; C4 – 100 percent. For example, the sympathisers would:

- Display associations with personalities known for their violent extremist views (C1): 'WARNING! Voting Will Negate Your Tawheed¹⁴ By Sheikh Omar Bakri Muhammad¹⁵ (may Allah release him)' [sic].
- Identify with symbols of known violent extremist groups on one's online profile (C2): 'Please dua to #FreeSheikhOmarBakri as he is due in court tomorrow for trial' [sic].
- Praise and defend violent extremist groups (C4): 'I feel honored by The Islamic State. The kuffar fear me when they see me in their streets' [sic].

Involvement in online community

For this factor, one out of four indicators appeared in more than 50 percent of this subsample: OC1 – 66 percent. For example, the sympathisers would:

Possess violent extremist documents, music, videos etc. on computer or mobile devices

¹⁴ Tawheed refers to the indivisible oneness concept of monotheism in Islam.

¹⁵ Omar Bakri Muhammad is a radical preacher from the United Kingdom. He is associated with radical groups such as Hizb ut-Tahrir and al-Muhajiroun.

(OC1): ‘18+ this is an Iraqi army video showing the absolute barbarity and depravity of #Obama allies Shia militia/Iraqi army’ [sic].

Individual-centric protective elements

For this factor, one out of four indicators appeared in more than 50 percent of this subsample: IP2 – 66 percent. For example, the sympathisers would:

Demonstrate a willingness to engage in discussions of ideology and the use of violence (IP2): ‘One shouldn’t go to extreme in takfir, but also the other side of the spectrum can’t be forgotten, to go to extremes in NOT making takfir’ [sic].

Comparing foreign fighters with sympathisers

After understanding how the factors and their associated indicators are mapped to the fighter and sympathiser samples, the authors examined the commonalities and differences between these two groups.

What are the commonalities between foreign fighters and sympathisers?

Several common factors were identified. As seen in Table 2, there are three factors of interest: perceived grievances (PG), intolerance towards multi-religious, multi-racial living (I), commitment to violent extremist groups (C), and involvement in online community (OC).

This is in line with research that highlights perceived grievance as a form of motivation that influences violent extremists’ radicalisation process (Borum, 2011; Neo et al., 2014), the lack of understanding and tolerance exhibited by violent extremists outside of their own group (Hussain & Saltman, 2014; Pressman & Ivan, 2016), the process through which violent

extremists may re-negotiate their identities within the violent extremist movement and become more supportive towards the movement (Bowman-Grieve, 2009; Hegghammer, 2013), and the role of the online community (Neo, Dillon, & Khader, 2016; Neumann, 2012).

Thus, this observation suggests that ISIS supporters [i.e., foreign fighter or sympathiser] would create tweets that display: (i) notions that highlight injustices perpetrated against their community, faith, or belief; (ii) signs of intolerance towards others, especially those who do not belong to their in-group; (iii) overt support for ISIS and its campaign to set up an Islamic State; and (iv) links or other accounts that propagate violent extremist ideologies, news or in-group favouritism.

Furthermore, factors that were completely absent from both the foreign fighter and sympathiser groups were found. These factors were: susceptible to influence (SI); negative social support (N); and online environment-centric protective elements (OP). The absence of these factors may be attributed to the difficulties involved in deciphering and identifying them, or that these factors are not relevant in the online detection of ISIS fighters and sympathisers.

What are the differences between foreign fighters and a sympathisers?

There are several factors that have the potential to distinguish the foreign fighters from the sympathisers. As highlighted in purple in Table 2, this is based on the observed differences in the way the factors and their associated indicators were mapped between the two groups. The five factors were: the knowledge and skill to commit violent extremist offences (K), redemption and the pursuit for significance (S), readiness to use violence (R), online relationship building with like-minded individual

(OR), and individual-centric protective elements (IP).

The authors further examined the frequency of tweets at which each indicator was being mapped. To do so, the total number of tweets that was coded under each factor for both groups was calculated – see Table 3.

A total of 622 tweets were posted by this sample of fighters and sympathisers. After these tweets were mapped against the indicators, 334 tweets were coded, accounting for 53.6 percent of the total number of tweets. The rest of the tweets could not be coded, as they did not fit in any of the 42 indicators. There was also a difference in the number of tweets coded for both groups. 183 and 151 tweets were coded for the fighter and sympathiser groups respectively.

To determine whether there was statistical difference between the fighters and sympathisers, an independent t-test¹⁶ was conducted to compare the mean number of tweets of these two groups. The results of the t-test suggested that only one statistically significant finding was found. As compared to sympathisers (mean = 1.3), foreign fighters (mean = 13.3) created more tweets that displayed their readiness to commit violence, $t(4) = 10.85, p = .000$.

In other words, the foreign fighters have a higher likelihood to tweet postings such as: ‘Jihad is the cure for all diseases #FACT’; ‘The moustache men in deir need to realise if needed we are not afraid to slaughter all of deir and turn its ground red if required. #Khilafa’ and

‘Running away from jihad will not save you from death. You can die as a coward or you can die as a martyr.’ The identification of this factor appears to be consistent with past research on how violent extremists would act on their radical beliefs and manifest the willingness to use violence to achieve their objectives in a given situation (Borum 2015; Kebbell & Porter, 2012; Lloyd & Dean, 2015). For example, based on an analysis of 30 jihadi attacks, Neo and colleagues (2014, p. 13) found that ‘the first significant feature (representing 86.66 per cent of the 30 jihadi attacks in this study) emphasises the motivation of the individual to commit an act of violence championed by terrorist groups’ political or religious agenda’.

Can we identify ‘Readiness to Use Violence’ in time?

The aim of this exploratory study was to compare ISIS foreign fighters versus sympathisers based on their social media postings on Twitter. It was revealed that the factor ‘readiness to use violence’ can be used to distinguish the foreign fighters from the sympathisers. This finding may hold implications for designing counter violent extremism measures.

At the fundamental level, it suggests that the detection of potential foreign fighters would be improved if online screening tools were programmed to identify this factor. As previously noted, the ‘loudest’ members on social media platforms may not, in fact, be the ones most likely to engage in violence, while the most passive members are not automatically the most peaceful. This endeavour to empiri-

¹⁶ Before interpreting the results of the t-test, there is a need to ensure that the difference between the two groups is meaningfully large, independent of whether the difference is statistically significant (Cohen, 1988). To do so, the effect size was calculated using Cohen’s *d* and was found to be large at .983.

Table 3. Independent t-test results

Factor	Foreign fighter (N = 3)			Sympathiser (N = 3)			T- Test
	Total tweets	Mean	SD	Total tweets	Mean	SD	
Perceived grievances (PG)	21	7.0	6.2	59	19.6	8.5	2.07, n.s.*
Intolerance towards multi-religious, multi-racial living (I)	25	8.3	1.5	54	18.0	14.4	1.15, n.s.*
Knowledge and skill to commit violent extremist offences (K)	3	1.0	.0	1	.3	0.5	2.00, n.s.*
Redemption and the pursuit for significance (S)	11	3.6	4.7	0	.0	.0	1.34, n.s.*
Susceptible to influence (SI)	0	.0	.0	0	.0	.0	-
Readiness to use violence (R)	40	13.3	1.5	4	1.3	1.1	10.85, p = .00
Commitment to violent extremist groups (C)	20	6.6	3.5	23	7.6	3.5	.34, n.s.*
Online relationship building with like-minded individual (OR)	36	12.0	16.4	1	0.3	0.5	1.22, n.s.*
Involvement in online community (OC)	27	9.0	7.0	6	2.0	2.6	1.62, n.s.*
Negative social support (N)	0	.0	.0	0	.0	.0	-
Individual-centric protective elements (IP)	0	.0	.0	3	1.0	.0	-
Online environment-centric protective elements (OP)	0	.0	.0	0	.0	.0	-

cally test and validate a list of factors to identify and decipher between online ‘noise’ (i.e., sympathisers) and offline action (i.e., foreign fighters) represents a basis for further study and examination. It also highlights what can be done to correctly identify sympathisers, who should be treated differently from foreign fighters who will indeed use violence to further the group’s cause. Given that law enforcement agencies have finite investigative resources, the ability to distinguish foreign fighters from sympathisers will be useful for law enforcement to determine whether or not a suspected violent extremism case should be prioritised for more investigation.

Currently, the Home Team Behavioural Sciences Centre identifies this factor (i.e., readiness to use violence) as one of three factors that Home Team officers should be trained to use to identify potential violent extremists. Officers are trained to ask:

Have you encountered anyone who:

- Supports the use of violence as a solution to achieve his/her political/religious violent extremist agenda?
- Expresses low tolerance and resentment towards multi-racial and multi-religious living?
- Indicates interest to travel and participate in a foreign conflict?

Furthermore, it is interesting to note that while the results were not significant, the sympathisers manifested individual-centric protective elements (e.g., ‘Read my disclaimer, I’m against terrorism and proscribed organizations’) that may have reduced their likelihood to transit from online to offline behaviours, and become foreign fighters. Thus, beyond merely grappling with when and how an individual becomes radicalised, there is also value in exploring protective factors that dissuade individuals from getting involved in the first place. This notion has been corroborated by the findings from the General Intelligence and Security Service [AIVD] of the Netherlands. In their 2012 analysis on jihadism on the Internet, it was suggested that most of the people lack the willingness, the knowledge, the expertise and the connections to become a violent extremist. This underscores the value of being cognizant of factors that influence one’s decision not to be involved in violent extremism.

From a methodological perspective, there is a dearth of violent extremism studies that have adopted the use of empirical data to drive conclusions (Schuurman & Eijkman, 2013). Thus, the use of sympathisers as a comparison group against the foreign fighter sample not only increases reliability and validity as the information collected is primary data, but also acts as a ‘proper’ control group. This is in comparison to many violent extremism studies where the violent extremists are compared against violent criminals (e.g., Cook, 2014) and students (e.g., Stankov, Higgins, Saucier, & Knežević, 2010). As there are distinct differences among these groups, the violent criminal and student populations may not serve as ideal comparison groups. Indeed, there are several funda-

¹⁷ The authors note that the conventional radicalisation research tends to over-focus on the identification of risk factors and one’s pathway into violent extremism.

mental differences to keep in mind in comparing violent criminals with violent extremists. For example, although prior criminal acts have been found to predict future offending (Monahan et al., 2001), no such correlation has been demonstrated among violent extremists. Furthermore, most violent extremists do not lack education, employment or have had troubled childhoods (Silber & Bhatt, 2007). They are in fact very 'normal' in comparison to the general population. Violent extremists also generally do not have a predisposition towards aggressive behaviour unlike other violent crime offenders (Pressman, 2009); violent extremists see violence as a viable means to achieve their agenda.

However, our findings comparing sympathisers with foreign fighters have to be interpreted with caution, as the generalizability of the findings is limited. There are a few limitations that must be taken into account. Firstly, this is an exploratory study with a small sample size. There is therefore a need to increase the sample of foreign fighters and sympathisers for future research. Secondly, it is important to recognise that these factors offer only a snapshot of an individual's beliefs at a particular moment in time, and regular assessment is required if law enforcement needs to portray a complete picture of the person of interest. Thirdly, such forms of online analysis are dependent on and restricted by the amount of information available (Egan et al., 2016). Thus, there is a need to move beyond Twitter and search for other social media platforms (e.g., Facebook, Instagram, Ask.fm, Tumblr, WordPress) that foreign fighters and sympathisers may use. Lastly, as Gill and colleagues (2017, p. 100) argue:

[T]here is no easy offline versus online violent radicalisation dichotomy to be drawn. It may be a false dichotomy. Plotters regularly engage in activities in both domains. Often their behaviours

are compartmentalised across these two domains ... A preoccupation with only checking online behaviours may lead an intelligence analyst to miss crucial face-to-face components of a plot's technical development or a perpetrators' motivations. (p. 100)

Thus, there is an essential need to complement these online assessments with offline information gathering.

In conclusion, the current study proposes a basis for future research in the field, as it is one of the first attempts to empirically explore and compare ISIS foreign fighters versus sympathisers based on their social media postings, and provides a unique contribution to the field of violent extremism.

About the Authors



Neo Loo Seng is a Principal Behavioural Sciences Research Analyst with the Home Team Behavioural Sciences Centre at the Ministry of Home Affairs, Singapore. For the past 10 years, Loo Seng has been specialising in the area of violent extremism, particularly in the fields of online radicalisation, online threat assessment, pre-attack warning signs, and psychology of violent extremism. He has presented at many international conferences, trained law enforcement officers, and published many research reports and journals on the topic of violent extremism. He is also the editor of *Combating Violent Extremism and Radicalisation in the Digital Era* (IGI Global, 2016). He is a member of the Online Radicalisation Research Community of Practice (ORRCOP) comprising Singaporean practitioners and subject matter experts involved in research related to online radicalisation. Loo is currently pursuing his Masters of Arts by Research degree in psychology at Nanyang Technological University on the personality profiles of violent extremists.

Dr. Joyce S Pang received her undergraduate training in psychology from Smith College, MA, USA, and her PhD in personality psychology from University of Michigan, MI, USA. As a personality psychologist, she is interested in the assessment of individual differences and in making finer distinctions between personality dimensions in order to increase theoretical understanding of how personality affects behaviour. In all her research, Joyce adopts a person x situation perspective to understand how individual differences predict different reactions within different social contexts, which in turn lead to important personal and social outcomes. Joyce S Pang is current Associate Professor and Head of Psychology at Nanyang Technological University.



Dr. Majeed Khader is the Chief Psychologist of Ministry of Home Affairs, Director of the Home Team Behavioural Sciences Centre, and concurrent Deputy Director of the Police Psychological Services Division. He plays a key role in directing and guiding research, training, and operational support of various behavioural sciences domains.

References

- Alam, F., Stepanov, E. A., & Riccardi, G. (2013). Personality traits recognition on social network – Facebook. Paper presented at the Workshop on Computational Personality Recognition, Italy.
- Back, M. D., Stopfer, J. M., Vazire, S., Gaddis, S., Schmukle, S. C., Egloff, B., & Gosling, S. D. (2010). Facebook profiles reflect actual personality, not self-idealization. *Psychological Science* 21(3), 372-374.
- Borum, R. (2011). Radicalisation into violent extremism I: A review of social science theories. *Journal of Strategic Security* 4(4), 7-36.
- Borum, R. (2015). Assessing risk for terrorism involvement. *Journal of Threat Assessment and Management* 2(2), 63-87.
- Bowman-Grieve, L. (2009). Exploring “Stormfront”: A virtual community of radical right. *Studies in Conflict & Terrorism* 32(11), 989-1007.
- Carter, J. A., Maher, S., & Neumann, P. R. (2014). #Greenbirds: *Measuring importance and influence in Syrian Foreign fighter networks*. London: ICSR.
- Cohen, J. (1988). *Statistical power analysis for the behavioural sciences 2nd edition*. New York, NY: Academic Press.
- Conway, M. (2007). Terrorist use of the internet and the challenges of governing cyberspace. In D., Myriam, V., Mauer, & F., Krishna-Hensel (Eds.), *Power and security in the information age: Investigating the role of the state in cyberspace*. London: Ashgate, 95-127.
- Cook, A. N. (2014). Risk assessment and management of group-based violence. Doctoral dissertation, Simon Fraser University, 2014. Retrieved from http://summit.sfu.ca/system/files/iritem1/14289/etd8437_ACook.pdf
- Dawson, L. L., Amarasingam, A., & Bain, A. (2016). Talking to foreign fighters: Socio-economic push versus existential pull factors. *Working paper series*, no.16-14. Canada: TSAS Canadian network for research on terrorism, security and society.
- Edwards, C., & Gribbon, L. (2013). Pathways to violent extremism in the digital era. *The RUSI Journal* 158(5), 40-47.
- Egan, V., Cole, J., Cole, B., Alison, L., Alison, E., Waring, S., & Elntib, S. (2016). Can you identify violent extremists using a screening checklist and open-source intelligence alone? *Journal of Threat Assessment and Management* 3(1), 21-36.
- General Intelligence and Security Service [AIVD]. (2012). Jihadism on the web: A breeding ground for jihad in the modern age. *The Hague: Algemene Inlichtingen en Veiligheidsdienst*.
- Gill, P. (2015). *Lone actor terrorists: A behavioural analysis*. New York, NY: Routledge.
- Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M., & Horgan, J. (2017). Terrorist use of the internet by the numbers. *Criminology & Public Policy* 16(1), 99-117.
- Kebbell, M. R., & Porter, L. (2012). An intelligence assessment framework for identifying individuals at risk of committing acts of violent extremism against the West. *Security Journal* 25(3), 212-228.
- Hegghammer, T. (2013). Should I stay or should I go. Explaining variation in western jihadists' choice between domestic and foreign fighting. *American Political Science Review* 1-15.
- Hussain, G., & Saltman, E. M. (2014). *Jihad trending: a comprehensive analysis of online extremism and how to counter it*. UK: Quilliam Foundation.
- Klausen, J. (2015). Tweeting the jihad: Social media networks of western foreign fighters in Syria and Iraq. *Studies in Conflict & Terrorism* 38(1), 1-22.
- Kosinskia, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the United States* 110(15), 5802.
- Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics* 33, 159-174.

- Lloyd, M., & Dean, C. (2015). The development of structured guidelines for assessing risk in extremist offenders. *Journal of Threat Assessment and Management* 2(1), 40-52.
- Mans, K., & Tuitel, R. (2016). Foreign fighters in their own words: Using YouTube as a source. The Netherlands: International Centre for Counter-Terrorism – *The Hague* (ICCT).
- Meloy, J. R., Roshdi, K., Glaz-Ocik, J., & Hoffmann, J. (2015). Investigating the individual terrorist in Europe. *Journal of Threat Assessment and Management* 2(3-4), 140-152.
- Monahan, J. (2012). The individual risk assessment of terrorism. *Psychology, Public Policy & the Law* 18, 167-205.
- Monahan, J., Steadman, H. J., Sliver, E., Applebaum, P. S., Robbins, P. C., Mulvey, E.P., Roth, L., Grisso, T., & Banks, S. (2001). Rethinking risk assessment: *The MacArthur study of mental disorder and violence*. New York: Oxford University Press.
- Neo, L. S., Dillon, L., & Khader, M. (2016). Identifying individuals at risk of being radicalised via the internet. *Security Journal*. Advance online publication. doi: 10.1057/s41284-016-0080-z.
- Neo, L. S., Dillon, L., & Tan, J. (2016). *Violent extremist cyber footprints: A guide to understanding and countering online violent extremism* (Rev. ed). Singapore: Home Team Behavioural Sciences Centre.
- Neo, L. S., Khader, M., Ang, J., Ong, G., & Tan, E. (2014). Developing an early screening guide for jihadi terrorism: A behavioural analysis of 30 terror attacks. *Security Journal*. Advance online publication. doi: 10.1057/sj.2014.44.
- Neumann, P. R. (2012). *Countering online radicalisation in America*. US: Bipartisan Policy Center.
- Pressman, E. (2009). Risk Assessment Decisions for Violent Political Extremism. *User Report 2009-02*. Ottawa: Public Safety Canada.
- Pressman, D. E., & Flockton, J. S. (2012). Calibrating risk for violent political extremists: The VERA-2 Structural Assessment. *The British Journal of Forensic Practice* 14(4), 237-251.
- Pressman, D. E., & Ivan, C. (2016). Internet Use and Violent Extremism: A Cyber-VERA Risk Assessment Protocol. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era*. Hershey, PA: IGI Global, 402-420.
- Schuurman, B., & Eijkman, Q. (2013). Moving terrorism research forward: The crucial role of primary sources. The Netherlands: International Centre for Counter-Terrorism – *The Hague*.
- Silber, M.D. and Bhatt, A. (2007). *Radicalization in the West: The Home Grown Threat*. New York: NYPD.
- Stankov, L., Higgins, D., Saucier, G., & Knežević, G. (2010). Contemporary militant extremism: A linguistic approach to scale development. *Psychological Assessment* 22(2), 246-258.
- The Soufan Group. (2015, December). *Foreign fighters: An updated assessment of the flow of foreign fighters into Syria and Iraq*. Retrieved from http://soufangroup.com/wp-content/uploads/2015/12/TSG_ForeignFightersUpdate3.pdf
- Vidino, L., & Hughes, S. (2015). *ISIS in America: From retweets to Raqqa*. US: The George Washington University.
- Weimann, G. (2004). www.terror.net: How modern terrorism uses the Internet. *Special Report No.116*. US: United States Institute of Peace.

The Seven Things You Need To Know About Lone-Actor Terrorism

By Dr. Paul Gill
 Department of Security and Crime Science
 University College London

Lone actor terrorists of various ideological hues provide the predominant terrorist threat in the West today. For the past seven years, I, along with several colleagues, have studied lone-actor terrorists from a number of different angles. This has involved both qualitative and quantitative research, open- and closed-source data and research on both the offenders and the offences themselves.

The purpose of this article is to synthesise the findings from this research. Broadly speaking, we have come to seven key conclusions. First, there is no socio-demographic profile. Second, generally somebody knew something in the build-up about the individual's motivations, planning and intent. Third, motivation does not centre purely around ideology. Fourth, the attacks are rarely sudden and impulsive but things may be changing. Fifth, lone-actor terrorists look and behave a lot like mass murderers. Sixth, mental health problems are common and complex within the offender sample. Finally, 'online radicalisation' is a misnomer. Below, I elaborate upon each of these key find-

ings with reference to various illustrative examples.

1. There is no socio-demographic profile

Although heavily male-oriented, there were no uniform variables that characterized all or even a majority of lone-actor terrorists. The sample ranged in age from teenagers to an individual who was 88 years of age at the time of his attack. Many were single but just as many were married or in a relationship. Some were PhD graduates, others high school drop-outs. Two-fifths had criminal convictions and the offences ranged from the very serious (e.g. homicide) to the very little. Thus, no clear profile emerged from the data. Even if such a profile were evident, however, an over-reliance on the use of such a profile would be unwarranted because many more people who do not engage in lone-actor terrorism would share these characteristics, while others might not but would still engage in lone-actor terrorism.

2. Generally somebody knew something

The evidence suggests that the assumed image of the lone actor terrorist conducting every aspect of his/her radicalization, attack planning and preparation without any aid or interaction is largely misguided. The true loners are few and far between. Although they engaged in the violence by themselves, most of the sample consumed and accepted a broad legitimating ideology and call to arms of others, were enabled by the provision of safe spaces to psychologically and physically prepare for engagement in violence, and a smaller number received some form of training or material support.

In the majority of cases, other individuals knew something concerning some aspect of the offender's grievance, intent, beliefs, or extremist ideology prior to the event or planned event. In 26.5 percent of cases, the offender produced letters or public statements prior to the event outlining his/her beliefs (but not necessarily his/her violent intent). This behaviour was largely confined to extremist forums. In 83.7 percent of the cases, other people were aware of the individual's grievance that spurred the terrorist plot, and in 87.8 percent, other individuals were aware of the individual's commitment to a specific extremist ideology. In 59.2 percent of the cases, family and friends were aware of the individual's intent to engage in terrorism-related activities because the offender verbally told them. Recipients included an imam, a son, friends, work colleagues, wives, sisters, and school friends. For 63.3 percent of the sample, there was an identifiable bystander to the individual's planning/preparation behaviours. These were typically individuals who witnessed concerning behaviours (e.g. seeing the offender looking at bomb-making manuals at work) but were not privy to the individual's specific plans. In 73.5 percent of cases, the offenders expressed a desire to hurt others. This

desire was communicated through either verbal or written statements. These findings suggest therefore that friends and family can play important roles in efforts that seek to prevent terrorist plots.

3. Motivation does not centre purely around ideology

On the surface, lone-actor terrorist attacks seem to defy explanation. The immediate aftermath of both phenomena is marked by drama, panic and an inevitable search for simple answers. In particular, there is an unerring tendency to reach for mono-causal master narrative explanations. The individual actor is either deranged, unbalanced, unhinged, disturbed, mad, crazy, nuts and unstable, or he/she is driven by a hateful ideology, radicalized, politically focused, inspired by some foreign 'entity', or determined to effect some social or political upheaval or policy change. In the days that follow an event such as these, the framing of the individual's motivation usually takes on one of these two narratives. The chosen narrative depends upon the easy availability of information regarding their ideological content, mental health history or personal background details.

Yet what we see from the analysis we offer here is that such attacks are usually the culmination of a complex mix of personal, political and social drivers that crystalize at the same time to drive the individual down the path of violent action. Whether the violence comes to fruition is usually a combination of the availability and vulnerability of suitable targets that suit the heady mix of personal and political grievances and the individual's capability to engage in an attack from both a psychological and technical capability standpoint. Many individual cases shared a mixture of unfortunate personal life circumstances coupled with an intensification of beliefs/grievances that later

developed into the idea to engage in violence. What differed was how these influences were sequenced. Sometimes personal problems led to a susceptibility to ideological influences. Sometimes long-held ideological influences became intensified after the experience of personal problems. This is why we should be wary of mono-causal master narratives (e.g. it was caused by mental illness). The development of these behaviours is usually far more labyrinthine and dynamic.

4. The attacks are rarely sudden and impulsive but things may be changing

The timeframe between deciding to conduct an attack and actually stepping out the door to conduct an attack varied between 3 months and over 2 years. To a large extent, the case studies also reflect the large number of roadblocks and hurdles that a lone-actor terrorist encounters and must overcome in the successful commission of an attack. Oftentimes, this requires abandoning a more ambitious original plan for something less complicated. These hurdles may reflect why terrorism has historically been largely a group-based phenomenon – the pooling of talent, resources, expertise and experience in a group setting likely helps mitigate the difficulties in successfully committing a terrorist attack. Such resources are absent for many lone-actor terrorists, which may help explain why lone-actor terrorism has an even lower base rate than group-based terrorism. The lengthy nature of many preparation phases (in terms of the number of steps and the time it took to complete them), may also mean that many more lone-actor terrorist plots are conceived of but are subsequently abandoned due to difficulties in financing, acquiring weaponry or developing reliable IEDs. Developing an understanding of these potential roadblocks, as well as how they function, may aid future investigations that seek to disrupt future potential lone-actor terrorist

plots.

In the absence of a group's cumulative human, financial, political and logistical capital, know-how and capability, lone-actor terrorist events are difficult to conduct in all but those using the most basic means. The results suggest that in many cases the development of a lone-actor terrorist attack occurs over a long period of time, but that this time can be lessened dramatically when individuals choose to conduct more technically primitive attacks.

5. Lone-actor terrorists look and behave a lot like mass murderers

Mass murderers look very similar to lone-actor terrorists, perhaps only differing in the ratio to which they are personally versus politically aggrieved. They display no discernable socio-demographic profile, generally somebody knows something about the plot, many but not all are socially isolated, they engage in a wide range of pre-crimes, and they are rarely sudden and impulsive. We sought to examine whether their 'radicalization' trajectory towards this act of violence was also similar. The analyses suggest that they share a lot in common with the results outlined elsewhere. This has a multiplicity of implications for early detection, threat management and possibly disruption. The job of intelligence analysts (be it for the police or intelligence communities) often involves assessing the scale of an individual's threat based on often fragmentary information.

The analyses above do not point toward one single behavioural profile from which risk assessments can be built but instead provide insight for the development and application of structured professional judgments in these cases. Finally, the results also highlight the fact that (a) in most cases there tends to be long-held risk factors but (b) they tend to be enabled in a force multiplier effect by much

more recent situational stressors and that (c) the trajectory into violence tends to be a lengthy process.

6. Mental health problems are common and complex

In Corner, Gill, and Mason's (2015) sample of 153 lone-actor terrorists, 1.3 percent experienced Traumatic Brain Injury (TBI), 0.7 percent drug dependence, 8.5 percent schizophrenia, 0.7 percent schizoaffective disorder, 2.0 percent delusional disorder, 0.7 percent psychotic disorder, 7.2 percent depression, 3.9 percent bipolar disorder, 1.3 percent unspecified anxiety disorder, 0.7 percent dissociative disorder, 1.3 percent Obsessive Compulsive Disorder (OCD), 3.3 percent Post-Traumatic Stress Disorder (PTSD), 0.7 percent unspecified sleep disorder, 6.5 percent unspecified personality disorder, and 3.3 percent autism spectrum disorder.

Three disorders exhibited a higher prevalence in the lone-actor sample than in the general population (schizophrenia, delusional disorder, autism spectrum disorders). Three disorders exhibited a lower prevalence in the lone-actor sample than in the general population (depression, sleep disorders, and learning disabilities). Both studies highlight the higher proportion of schizophrenia within their samples compared to the wider population. It is important to note, however, that neither sample is representative of the vast majority of terrorists. Whilst foreign fighters and lone-actors hold much of the media's attention right now, they are still in the vast minority compared to terrorists globally and across history.

Corner and Gill (2015) utilized a sample of 119 lone-actor terrorists and investigated whether certain behaviours were more likely to co-occur with certain diagnoses than others. Those diagnosed with schizophrenia and associated

disorders were the only diagnostic group to be significantly associated with previous violent behaviour and this supports past research in the general violence literature. Negative associations were also found between personality disorders and autism and having a spouse/partner involved in a terror movement, which may be indicative of not having a spouse due to the detrimental nature of these disorders.

We also found that those who were mentally disordered were just as (and in some cases more) likely to engage in a range of rational pre-attack behaviours as those who were not. Mentally disordered offenders were more likely to express violent desires, seek legitimization for their intended actions, stockpile weapons, train, carry out a successful attack, kill and injure, discriminate in their targeting, and claim responsibility. Most of these traits are typically viewed as rational behaviours and essential for success.

7. 'Online radicalisation' is a misnomer

The growth of the Internet did not correlate with a rise in lone-actor terrorist activity annually from 1990 to 2011. However, there has been a growing trend among lone-actors to make use of the Internet. In other words, while the Internet has not caused a growth in numbers of lone-actor terrorists, it has altered their means of radicalization and learning. The Internet therefore acts as a substitute for other factors such as intelligence gathering and attack planning, but not necessarily as a force enabler. Within the sample, younger offenders were significantly more likely to engage in both virtual learning and virtual interaction than older offenders. Also, the non-U.S. based offenders were significantly more likely to learn through virtual sources. This may be a function of the U.S. offenders having a greater access to firearms and therefore not needing to go online. Interestingly, offenders who in-

teracted virtually with co-ideologues were significantly less likely to successfully carry out a violent attack. Similarly, offenders who prepared for an attack using virtual sources were significantly less likely to kill or injure (despite being significantly more likely to plot an attack against indiscriminate soft targets).

The use of the Internet was largely for instrumental purposes whether it be pre-attack (e.g. surveillance, learning, practice, communication) or post-attack (e.g. disseminating propaganda). In criminological terms, these activities were cyber-enabled rather than cyber-dependent. There is little-to-no evidence to suggest that the Internet was the sole expla-

nation that got actors to the point of deciding to engage in a violent act. Instead, it was just one factor amongst many that helped crystallise motivation, intent and capability at the same time and place. Evidence further suggests that many went online not to have their beliefs changed but rather reinforced.

Finally, a significant positive correlation existed between those who virtually interacted with co-ideologues and those who interacted with co-ideologues face-to-face. Radicalization (at least for lone actors) is not a dichotomy of either offline or online, but rather an interaction with others versus no interaction with others dichotomy.



About the Author

Dr. Paul Gill is a senior lecturer in Security and Crime Science at University College London. He was previously a postdoctoral research fellow at the International Center for the Study of Terrorism at Pennsylvania State University. He has over 50 publications on the topic of terrorist behaviour. He has conducted research funded by the Office for Naval Research, the Department of Homeland Security, DSTL, the European Union, the National Institute of Justice, CREST and MINERVA. Collectively, these grants have been worth over 9 million euro. These projects focused upon various aspects of terrorist behaviour including the IED development, creativity, terrorist network structures and lone-actor terrorism. His doctoral research focused on the underlying individual and organizational motivations behind suicide bombing. This piece of research won the Jean Blondel Prize for the best Ph.D. thesis in Political Science in Europe for 2010. He has published in leading psychology, criminology and political science journals.

References

- Alrajeh, D. and Gill, P. (2015). A Logic-Based Approach to Understanding Lone-Actor Terrorism. *Technical Communications of International Conference on Logic Programming (ICLP2015)*: Cambridge University Press, 2015.
- Bouhana, N., Malthaner, S., Schuurman, B., Lindekilde, L., Thornton, A. and Gill, P. (Forthcoming). Lone-Actor Terrorism: Radicalisation, Attack Planning and Execution, in the *Routledge Handbook of Terrorism and Counterterrorism*, A. Silke (ed.). London: Routledge.
- Corner, E. and Gill, P. (2015). A False Dichotomy? Lone Actor Terrorism and Mental Illness. *Law and Human Behavior* 39(1):23-34.
- Corner, E. and Gill, P. (2017). Is There a Nexus Between Terrorist Involvement and Mental Health in the Age of the Islamic State? *The CTC Sentinel* 10(1):1-10.
- Corner, E., Gill, P. and Mason, O. (2016). Mental Health Disorders and the Terrorist: A Research Note Probing Selection Effects and Disorder Prevalence. *Studies in Conflict and Terrorism* 39(6): 560-568.
- Gill, P. (2015). Towards a Scientific Approach to Identifying and Understanding Indicators of Radicalization and Terrorist Intent: Eight Key Problems. *Journal of Threat Assessment and Management* 2(3-4): 187-191.
- Gill, P. (2015). *Lone-Actor Terrorists: A Behavioural Analysis*. London: Routledge.
- Gill, P. and Corner, E. (2013). Disaggregating Terrorist Offenders: Implications for Research and Practice. *Criminology and Public Policy* 12(1): 93-101.
- Gill, P. and Corner, E. (2015). Lone-Actor Terrorist Use of the Internet & Behavioural Correlates. In *Terrorism Online: Politics, Law, Technology and Unconventional Violence*, L. Jarvis, S. Macdonald and T. Chen (eds.). London: Routledge.
- Gill, P. and Corner, E. (2016). "Lone-Actor Terrorist Target Choice". *Behavioral Sciences and the Law* 34(5): 693-705
- Gill, P. and Corner, E. (2017). There and Back Again: The Study of Mental Disorder and Terrorist Involvement. *American Psychologist* 72(3): 231-241.
- Gill, P., Corner, E., and Thornton, A. (2015). What are the roles of the Internet in terrorism? *Measuring Online Behaviours of convicted UK terrorists*. A Report for the European Union.
- Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M., and Horgan, J. (2017). Terrorist Use of the Internet by the Numbers: Quantifying Behaviors, Patterns & Processes. *Criminology and Public Policy* 16(1):99-117.
- Gill, P., Horgan, J., and Deckert, P. (2012). *Tracing the Motivations and Antecedent Behaviors of Lone-Actor Terrorism. Pennsylvania*: International Center for the Study of Terrorism.
- Gill, P., Horgan, J., and Deckert, P. (2014). Bombing Alone: Tracing the Motivations and Antecedent Behaviors of Lone-Actor Terrorists. *Journal of Forensic Sciences* 59(2):425-435.
- Gill, P., Horgan, J., Corner, E. and Silver, J. (2016). Risk Factors and Lone Actor Violent Events: The Problems of Low Base Rates and Long Observational Periods. *Journal of Threat Assessment and Management* 3(3-4):165-173.
- Gill, P., Silver, J., Horgan, J., and Corner, E. (Forthcoming). Shooting Alone: The Pre-Attack Experiences and Behaviors of U.S. Solo Mass Murderers with Implications for Threat Assessments. *Journal of Forensic Sciences*.
- Horgan, J., Gill, P., Bouhana, N., Silver, J., Corner, E. (2016). *Across the Universe? A Comparative Analysis of Violent Radicalization Across Three Offender Types with Implications for Criminal Justice Training and Education*. A Report for the National Institute of Justice.
- Meloy, J.R. and Gill, P. (2016). The Lone Actor Terrorist and the TRAP-18. *Journal of Threat Assessment and Management* 3(1): 37-52.
- Schuurman, B., Bakker, E., Gill, P., and Bouhana, N. (Forthcoming). Lone Actor Terrorist Attack Planning and Preparation: A Data-Driven Analysis. *Journal of Forensic Sciences*.



About the Home Team Academy

The Home Team Academy's mission is to develop leaders, enable the Home Team Transformation and drive the transformation of the Home Team's training and learning capabilities to keep Singapore safe and secure. It aspires to be a globally recognised Asian safety and security corporate university.