# Asian Journal of Public Affairs

CONTENTS


**Editor's Note**
Addressing the future of human well-being and security 01
*Joanne Yoong, Helena Legido Quigley & Tikki Pangestu*

**Research Articles**
Singapore's Role and Contribution in Health Globally: A Qualitative Study Exploring Perspectives of Global Health Actors in Southeast Asia 04
*Joel Jun Kai Koh, Matthew Godfrey Reinert, Fiona Leh Hoon Chuah, Joanne Su-Yin Yoong, Francisco Cervero-Liceras, Victoria Haldane, Suan Ee Ong, Kee Seng Chia1, & Helena Legido-Quigley*

Protecting the Vertical Space of Cities: Perspectives for Singapore 27
*Muhammad Faizal Bin Abdul Rahman*

Fintech and the Future of Finance 52
*James Guild*

The Era of Ubiquitous Listening: Living in a World of Speech-Activated Devices 66
*Jennifer Yang Hui & Dymples Leong*

Exploring a New Approach to the Business Continuity Management Training Practices by Singapore Hotels to Manage the Terrorist Threat 85
*Kevin Wee*


Lee Kuan Yew School of Public Policy

NUS National University of Singapore



ISSN 1793-5342

Volume 10 | Issue 1 | 2017
Special Issue for the Raffles Dialogue 2017

# Asian Journal of Public Affairs

Lee Kuan Yew School of Public Policy

NUS National University of Singapore

## GLOBAL PUBLIC POLICY NETWORK

The Global Public Policy Network (GPPN) is a partnership between Columbia University (USA), Fundacao Getulio Vargas-EAESP (Brazil), University of Tokyo (Japan), Hertie School of Governance (Germany), Lee Kuan Yew School of Public Policy (Singapore), Institute of Public Affairs at LSE (UK) and Sciences Po, Paris (France). The GPPN is global in two ways: the global spread of its members and its subject focus on emerging global trends in public policy.

The mission of GPPN is to address the most pressing public policy challenges of the 21st century and, as a result, to have policy impact, to be influential in public policy education and training, and to be innovative in teaching and research. For further information please visit www.gppn.net.

## CALL FOR PAPERS

The Asian Journal of Public Affairs accepts manuscripts of original research articles (6,000-7,000 words excluding abstract and bibliography), book reviews (multiple or single), and commentaries (1,500 words maximum). Contributions are accepted on a rolling basis. Please email your manuscripts to our email address (**ajpa@nus.edu.sg**). Citations must follow the Chicago Manual of Style. Please refer to "Author Guidelines" on our website for more details.

Should you need more information, please feel free to contact the Editorial Board or visit our website. Please also subscribe to *Asian Journal of Public Affairs* on our website to receive newsletters.

# Asian Journal of Public Affairs

**Vision**
The Asian Journal of Public Affairs (AJPA) seeks to be the choice journal for scholars and practitioners interested in public affairs in the Asia-Pacific region. The journal endeavours to become the leading intellectual voice on Asia.

**Mission**
The Asian Journal of Public Affairs (AJPA) publishes policy-relevant research written by and for scholars and practitioners around the world who are interested in the Asia-Pacific region. The journal encourages both young and senior scholars and practitioners to reflect on and study the Asian public sphere from an interdisciplinary lens.

**Aims and Scope of Journal**
The Asian Journal of Public Affairs (AJPA) is the flagship student journal of the Lee Kuan Yew School of Public Policy (LKYSPP). It is a peer-reviewed publication featuring articles by scholars and practitioners on public affairs issues in the Greater Asia including the Middle East, Central and South Asia, and the Asia-Pacific region. Published on a bi-annual basis, AJPA seeks to influence public policy-making in Asia through interdisciplinary policy-relevant research. Print circulation is targeted not only to academic audiences but also to civil society and government organizations. The scope of Public Affairs includes, but is not limited to, Public Policy (including sectoral policies), Public Administration and Management, International Security, International Political Economy, Social and Political Sciences and Economics. Each issue features scholarly and practitioner-based research articles, field reports, commentaries, and book reviews. Articles may be quantitative and/or qualitative, national or cross-national. Preference is given to contributions which have accessible and clearly articulated policy implications.

# Asian Journal of Public Affairs

## EDITORIAL TEAM



## ACKNOWLEDGMENTS

**School Advisory Board**
Professor Michael Howlett
Associate Professor Eduardo Araral Jr.
Professor Mukul Asher
Dr. Suzaina Kadir
Associate Professor Zeger van der Wal

**International Advisory Board**
Professor Frances Berry
Professor Evan Berman
Professor Takashi Inoguchi
Professor Qingguo Jia
Professor Yijia Jing
Professor Jun Ki Kim
Professor James Perry
Professor Alasdair S. Roberts
Professor Allan Rosenbaum
Professor Diane Stone
Professor René Torenvlied
Professor Kaifeng Yang
Professor Yang Zhong
Professor Amitav Acharya

**Print**
Markono Print Media Pte Ltd

# ASIAN JOURNAL OF PUBLIC AFFAIRS

**Volume 10 Issue 1 2017**

CONTENTS

**Editor's Note**
Addressing the future of human well-being and security 01
*Joanne Yoong, Helena Legido Quigley & Tikki Pangestu*

**Research Articles**
Singapore's Role and Contribution in Health Globally: A Qualitative Study Exploring Perspectives of Global Health Actors in Southeast Asia 04
*Joel Jun Kai Koh, Matthew Godfrey Reinert, Fiona Leh Hoon Chuah, Joanne Su-Yin Yoong, Francisco Cervero-Liceras, Victoria Haldane, Suan Ee Ong, Kee Seng Chia1, & Helena Legido-Quigley*

Protecting the Vertical Space of Cities: Perspectives for Singapore 27
*Muhammad Faizal Bin Abdul Rahman*

Fintech and the Future of Finance 52
*James Guild*

The Era of Ubiquitous Listening: Living in a World of Speech-Activated Devices 66
*Jennifer Yang Hui & Dymples Leong*

Exploring a New Approach to the Business Continuity Management Training Practices by Singapore Hotels to Manage the Terrorist Threat 85
*Kevin Wee*

NOTE FROM THE EDITORS

# Addressing the future of human well-being and security: A Special Issue for The Raffles Dialogue 2017

*Joanne Yoong, Helena Legido Quigley & Tikki Pangestu*


This special issue of the AJPA is a companion to the Raffles Dialogue 2017, a forum which brings global thought leaders together in Singapore to discuss the future of human well-being and security. As we approach this year's Raffles Dialogue, now more than ever, assaults and demands from multiple directions force us to reflect on a complex range of inter-connected political, economic, financial, social and environmental factors and the policy responses or strategies that are most likely to help ensure continued international cooperation and goodwill at the highest levels.

Three threats which we believe are of key importance may warrant more considered discourse and debate.

First, global institutions are in flux and in need of reform while globalisation marches on. From the global financial crisis in 2008, to the continuing impasse, and setbacks, on climate change mitigation, to the leadership failure in dealing with the Ebola crisis, and to the ongoing epidemic of chronic diseases, many are perceiving a failure of global governance and asking 'are global institutions up to the task?', are they still 'fit for purpose' to achieve the targets of the Sustainable Development Goals (SDGs)? At the same time, the raise of nationalism, international geopolitical tensions, internal conflict, the refugee crisis, extremism and instability continue which span military, security, social and economic dimensions. The hegemony of the west continues to be challenged by the emerging powers, particularly China and Russia, with new players such as the MIST countries emerging as important future actors (Mexico, Indonesia, South Korea and Turkey) and other countries, such as Japan and Thailand, playing a crucial role in global health diplomacy. A new round of trade wars appears to be brewing with conflicting and overlapping initiatives being championed by vested interests in different regions of the world. Multilateral institutions and governments are busily engaged in implementing the SDGs after the Millennium Development Goals (MDGs) ended in 2015. While the SDGs focuses on the laudable aim of 'sustainable development', the key question is 'can the current architecture of global institutions deliver?'

Second, while technology also marches on relentlessly and impressively, core philosophical and ethical questions about the generation and distribution of health and well-being in society remain unanswered. As advances in biomedical technology are allowing us to live longer than our parents and grandparents, existing concerns about equity, ethics, fairness and waste persist, while new concerns emerge over cybersecurity, confidentiality and paucity of data in both the developed and the developing world.

Finally, our planet is at greater risk than ever. Extreme climate events resulting in floods, droughts and other natural disasters continue to plague the world while continued inaction stalls efforts and pledges to deal with the ill effects of climate change. Despite strong evidence that by 2100 the global average temperature will probably be more than 4°C above preindustrial levels, and the existence of a United Nations Framework Convention on Climate Change, the many climate change conferences on this critical issue have so far failed to conclude a binding global treaty to mitigate the effects of climate change. The recent US withdrawal from the Paris Agreement on reducing CO2 emissions is likely to exacerbate the problem.

To mitigate these threats, first, we need to design new institutions, or revamp current institutional arrangements, seek novel modes of financing, promote international solidarity, and design people centred polices, with clear prioritization of objectives and goals. Second, it is clear that multilateral institutions and multilateralism must work hand-in-hand with nation states and respect the ideals of sovereignty and national responsibility. Third, in all our future efforts we must acknowledge the value and importance of local knowledge, culture, community and regional solidarity. Finally, whilst global institutions are a complex system, with multiple interests, power relationships and with a range of challenges for coordination and accountability, there is a need to assure strong and renewed leadership while making sure we “do not leave anyone behind”.

Reflecting on the role of Singapore, while Singapore is a small country that cannot be considered an economic powerhouse in absolute terms, it has critical assets that allow it to play a pivotal role in some areas. Building on its strong and high quality education system, highly-ranked tertiary academic institutions and commitment to research, it has also played an important leadership role in convening platforms for debating and discussing important global and national issues. In this volume of the AJPA, we present papers selected from young researchers’ submissions to the Raffles Dialogue that reflect the key themes above.

Firstly, a qualitative study explores Asia Singapore's contribution in health globally from the perspective of global health actors in Southeast Asia. Joel Koh, Matthew Reinert, Fiona Chuah and their coauthors argue that Singapore’s role as a leader in biomedical innovation has the potential to further develop for the benefit of the region.

In the second and third article in this volume, Muhammad Faizal Bin Abdul Rahman and Kevin Wee analyse the regulatory and operational implications of emerging threats to security for Singapore for public and private stakeholders. The former evaluates policy considerations that arise from the increasingly vertical nature of the city landscape, while the latter examines the impact of terrorism on business continuity for the hotel industry.

The last two articles address the benefits and costs of new technology and the evolving balance between promoting innovation and managing personal and societal risks. Jennifer Yang Hui and Dymples Leong explore new challenges to privacy in an era of "ubiquitous listening" devices, while James Guild reviews regulatory approaches to new financial technologies that continue to maintain appropriate oversight while enabling increases in access and inclusion.

It is our hope that these articles and the Raffles Dialogue more broadly, will contribute to the much needed continuing discourse on the future of human well-being and security, as well as our collective search for new policy solutions in the coming years.

RESEARCH ARTICLE

# Singapore's Role and Contribution in Health Globally: A Qualitative Study Exploring Perspectives of Global Health Actors in Southeast Asia

***Joel Jun Kai Koh[1]*, Matthew Godfrey Reinert[1]*, Fiona Leh Hoon Chuah[1]*, Joanne Su-Yin Yoong[1], Francisco Cervero-Liceras[1], Victoria Haldane[1], Suan Ee Ong[1], Kee Seng Chia[1], Helena Legido-Quigley[1,2]***

AJPA Asian Journal of Public Affairs

**Keywords**: Singapore, role, contribution, global health, Southeast Asia

**Suggested Article Citation**: Koh, Joel Jun Kai et al. 2017. "Singapore's Role and Contribution in Health Globally: A Qualitative Study Exploring Perspectives of Global Health Actors in Southeast Asia." *Asian Journal of Public Affairs* 10(1): p. 3–26.

http://dx.doi.org/10.18003/ajpa.20178

ISSN 1793-5342 (print); ISSN 2382-6134 (online),  Published by Lee Kuan Yew School of Public Policy, National University of Singapore

**ABSTRACT**

*In line with the recent adoption of the Sustainable Development Goals, global health has grown increasingly relevant in Southeast Asia (SEA), with the proliferation of new actors and growing interest in global health issues. In SEA, Singapore has emerged as a developed nation with the capabilities and resources to be a powerful force of change for progress in global health. The aim of this paper is to explore the perceptions of global health actors in SEA on Singapore's role and contributions to the global health landscape. Twenty-five semi-structured interviews were conducted with participants from the SEA region with global health expertise and experience. Key-informants were recruited from a range of international and local health institutions across public and private sectors. Thematic analysis was conducted to identify emergent themes. Findings suggest that Singapore is perceived as being successful in achieving the Millennium Development Goals (MDGs), in its progress in healthcare and in its ability to exercise good governance. Obstacles that hampered Singapore's ability to do more in global health were linked to its pragmatic priorities focusing on domestic health. The findings suggest a myriad of ways in which*

[1] Saw Swee Hock School of Public Health National University of Singapore, Tahir Foundation Building, 12 Science Drive 2 #10-01 Singapore 117549

[2] London School of Hygiene & Tropical Medicine, Keppel St, Bloomsbury, London WC1E 7HT, UK

* Co-first authors

Corresponding Author: Helena Legido-Quigley (Email: ephhlq@nus.edu.sg)

*Singapore can expand its role in health globally by leveraging the strength of its academic institutions, good structures of governance, and influence in the region. Such efforts are perceived to yield practical benefits in bolstering Singapore's security, economy and foreign relations, while enabling the state to contribute towards more charitable goals in reducing the global burden of disease. Drawing on our findings and supporting literature, a more comprehensive multidisciplinary research project examining Singapore's existing global health footprint in various sectors and its potential to contribute more in global health could be beneficial.*

## INTRODUCTION

In September 2015, 17 Sustainable Development Goals (SDGs) were adopted by governments globally to continue expanding the work of the Millennium Development Goals (MDGs). The SDGs listed a set of universal goals to be attained, including one focusing on ensuring the health and well-being for all persons (UNDP 2017). The implementation of the SDGs marks a propitious time to critically examine the extent to which global health governance is grounded in the right to health, as well as the readiness of our existing global health architecture and its various stakeholders to work towards these goals (Van de Pas et al. 2017; Hoffman et al. 2015).

The fundamental way in which global health is conceived determines the health problems to prioritize and the actors involved (Frenk et al. 2014). In a global health landscape of 'complex interdependence', both state and non-state entities rely on each other for effective governance to achieve universal goals (Frenk et al. 2014, Lamy and Phua 2012). As underscored by the Lancet-University of Oslo Commission on Global Governance for Health, global health governance demands the need to consider forces and sectors beyond the global health system and their influences on health (Ottersen et al. 2014). For instance, during the recent Ebola crisis, the Independent Panel on Global Response to Ebola called for urgent reform of the governance and stewardship structures in global health to clarify the roles and responsibilities of all national, regional, and international actors spanning across the public, private and not-for-profit sectors (Moon et al. 2015). In this regard, national governments are duty-bound to ensure credible, efficient, and equitable decision-making and action for global health, as prioritizing the right to health over other transnational activity is a global political responsibility (Ottersen et al. 2014).

In 2003, Southeast Asia (SEA) was faced with a potential Severe Acute Respiratory System (SARS) epidemic, which highlighted the weakness of existing regional health collaborations (Chongsuvivatwong et al. 2011). Several authors pointed to the difficulty in engaging SEA in global health issues, due to the challenges in balancing governance and sovereignty (Lamy and Phua 2012), and finding a common approach to engage global health issues amid regional political diversity (Tan et al. 2012). This predicament is exacerbated due to health determinants such as migration and food security, which have become more prominent in the region (Chongsuvivatwong et al. 2011).

As a high-income country (World Bank 2017) with the highest Human Development Index value in the region (UNDP 2016), Singapore is a key player both on the global stage and within ASEAN. In the most recent Lancet report measuring health-related SDGs in 188 countries worldwide, Singapore was among the top scorers in achieving its global health targets (Lim et al. 2016). In the 2015 Global Burden of Disease Study, Singapore scored higher than other ASEAN countries on the Healthcare Access and Quality Index (Barber et al. 2017). This is testament to the success of Singapore's healthcare system, and its potential to become a force of change for progress as a global health hub. For this reason, Jahncke et al. (2010) sought to explore the challenges and opportunities for Singapore in the field of global health. However, to our knowledge, no studies have explored this further since.

Internationally, developed countries are beginning to recognize the importance of mapping their footprint in health to strengthen their position as global leaders, as shown by reports such as 'The UK's Contribution to Health Globally' (Hasan et al. 2015). Similarly, this paper aims to explore the perceptions of global health actors in SEA on Singapore's role and contributions to global health. The information generated from this exploratory study will be useful for stakeholders in health and other sectors within Singapore to establish further policy priorities in global health. This qualitative study also builds upon the pioneering work of Jahncke et al. (2010) who reviewed the training, funding, and resources of Singapore to produce a 'roadmap' of how Singapore could engage with global health. The authors in their study assert that Singapore can benefit from contributions in global health through the application of the five metaphors of global health policy conceptualised by Stuckler and Mckee (2008), namely global health as 'security', 'investment', 'foreign policy', 'charity', and 'public health'. These metaphors will therefore be used as analytical tools to address the aim of this study.

## METHODS

### *Participants and Sampling*

This study, carried out from January 2016 to April 2017, was part of a larger study exploring the global health architecture in Asia. In this larger study, purposive sampling was adopted to identify participants from a variety of sectors, countries and institutions, all of whom were involved in global health. These participants were identified from regional global health conferences or events that the researchers attended and through the research team's professional contacts. Additional participants were then recruited through snowball sampling techniques, which involved asking interviewees to nominate individuals whom they knew with knowledge and experience relevant to the study. The final pool of 25 participants represented various actors involved in global health, ranging from government ministries, UN agencies, civil society organizations, global health donors, academia, and the private sector. Participants were from Singapore, the Philippines, Cambodia, Myanmar, India and Thailand, comprising consultants, senior-level managers, professors and healthcare professionals. 20 individual semi-structured interviews and two natural group discussions, of two and three individuals respectively, were conducted. Each

interview lasted between 60 to 90 minutes and were conducted face-to-face or via Skype. Participants' characteristics are presented in Table 1. Local NGOs refer to entities organized at the local or national level of the participant's country. Participants whose country of origin was classified as regional or global are those that have substantial experiences across multiple countries in the SEA region or globally.

**Table 1: Characteristics of study participants**

| *Total Number of Participants* | *N = 25* |
|---|---|
| *Organization Type* | |
| UN | 8 |
| Academia | 4 |
| Government | 3 |
| Private Enterprise | 4 |
| International NGO | 2 |
| Local NGO | 2 |
| Regional NGO | 1 |
| Public Private Partnership | 1 |
| Multilateral Donor | 1 |
| *Countries* | |
| Myanmar | 8 |
| The Philippines | 4 |
| Singapore | 5 |
| Thailand | 3 |
| Cambodia | 1 |
| India | 1 |
| Regional | 2 |
| Global | 1 |

### *Ethical Approval*

Ethical approval was obtained from the National University of Singapore Institutional Review Board (NUS-IRB). Each participant was provided with an information sheet with study details. Signed consent was obtained for participation in the study and for permission to be audio-recorded. Participants were given opportunities to ask questions and express any concerns. Audio recordings were anonymised prior to transcription to protect participants' identities. Interview materials were stored securely and in accordance with NUS-IRB's policies and requirements. Participant names and identifying data were removed from all documents to maintain confidentiality. Each participant was also provided the option of not being quoted, even anonymously, in any subsequent publications. Participants could refuse to answer any questions or withdraw from the study at any point. Interview locations were private and comfortable for the participants.

### *Analysis*

This study follows an interpretative approach to explore participants' perceptions relating to Singapore's role and contributions in health globally. All audio

recordings were transcribed verbatim. Transcripts were coded using an inductive approach and the research team thematically analyzed the data using QSR NVIVO11, a qualitative data analysis software, to identify emergent themes and subthemes. Regular team discussions were held to discuss findings and deviant cases. Recruitment of participants ceased when researchers agreed that thematic saturation was achieved.

## RESULTS

This paper presents the issues reflecting our participants' perceptions on Singapore's role and contributions in global health. We describe the emergent themes on Singapore's current successes in global health; the challenges Singapore faces in expanding its efforts in global health; the potential additional roles of Singapore in this area; and the benefits and readiness of Singapore to increase its role in global health. Within these themes and subthemes, several key findings were elucidated (Table 2).

**Table 2: Key Themes and Findings as Reported by Participants**

| *Key Themes* | *Sub-themes* | *Key Findings* |
|---|---|---|
| **Perceptions of Singapore's successes in health globally** | Research and Education | • Singapore has significant accomplishments and contributions in the academic and research sector |
| | | • Singapore's successes are attributable to its long-term investments in human capital |
| | | • Singapore has contributed significantly in the capacity building of the younger generation from the region in the health sector through training and education |
| | | • Singapore is an attractive location for research given its advances in technology, infrastructure and expertise in healthcare |
| | | • Singapore's government is very supportive of its academic sector |
| | Health outcomes and access | • Singapore is a success in its achievements of the MDGs and in its progress towards Universal Health Coverage |
| | Good Governance | • Singapore's success is attributable to its political stability and the overall good governance |
| **Singapore's hesitation to play a greater role in global health** | Singapore's priorities | • Singapore's economic pragmatism is perceived to be key in shaping priorities in policy-making |
| | | • Singapore places more focus on pandemic preparedness and in combatting infectious diseases due to the potential threats on national security and economic stability |
| | | • Singapore and countries regionally frequently face competing priorities between health and other sectors |
| | | • Singapore's priorities focus primarily on local needs |

| | | |
|---|---|---|
| | Difficulties contributing to global health development | • Health policy and planning remains focused on domestic issues, a common phenomenon in Southeast Asia |
| | | • Richer countries like Singapore are perceived to be the ones to bear the brunt of the costs in global health development, with little return on investment |
| | | • Singapore is perceived to have never been on the receiving end of global health development |
| **Perceptions of Singapore's potential role in global health** | Greater expectations on Singapore despite its success | • Singapore has the ability to do more given its expertise, capacity and thriving economy |
| | | • Singapore is considered proactive in disaster response and global health security, but could take up a greater leadership role regionally and contribute to health systems strengthening |
| | | • The success of Singapore's healthcare system is partly due to the large in-flow of skilled healthcare professionals from the region. In return, there is an expectation for Singapore to contribute more in health to its neighbours |
| | Singapore could further increase its role in academia | • Singapore's academic expertise and infrastructure could be further harnessed for global health through a leadership role |
| | | • There is a need for further contributions through academic dialogues to inspire change and greater contribution in global health |
| | Singapore can leverage on its expertise to seed larger projects | • Singapore can leverage on its expertise and technology to develop innovative pilot interventions that can be scaled up by other countries and entities |
| | Filling the health gap in ASEAN | • Singapore could take the lead in addressing health gaps within ASEAN including integrating health and other sectors, and encouraging regional engagement to create an ASEAN 'health community' |
| **Perceived benefits if Singapore increases its role in health globally and Singapore's willingness to do so** | Practical benefits to increase its role | • Engagement in global health is beneficial for foreign diplomacy and soft power, and could be a stepping stone to solving other transnational issues |
| | | • Efforts in global health facilitates regional cooperation which benefits Singapore as a small country |
| | | • There is a need for Singapore's health workforce to engage in sectors beyond health globally |
| | Perceptions on Singapore's willingness to increase its role | • Perceptions were generally mixed. Some saw Singapore as willing to take up more leadership in global health, while others felt there is a lack of political will |
| | | • It is perceived that once Singapore decides to play a greater role in global health, it will be fully committed in doing it well |

### *Perceptions of Singapore's Successes in Health Globally*

*Research and Education*

Based on participant narratives, one of Singapore's key successes in global health is in its accomplishments in the academic and research sector. Internationally, Singapore's universities have achieved competitive rankings and maintained a positive reputation for education and research. Some participants attributed this success to the country's investment in human capital over the years, as exemplified in this quote:

> *"NUS is a pretty good institution, now it's one of the top-rated. That's because Singapore, like Hong Kong, has just invested huge […] because they seek and see the human capital issues as important, […] the fact that they developed this Duke-NUS thing for graduate medical school […] these are all very deliberate strategies to open, change, bring people in, establish the connection, in a very Singaporean way."*
> *(Regional, UN)*

Through investments in human capital, some participants pointed out that Singapore now possesses a cadre of health care workers and human resources with good knowledge, skills, and technical expertise in health. Over the years, this has translated into capacity-building efforts in the form of education and training of younger generations, many of whom originate from countries around the region and globally. Many participants viewed this as a key contribution of Singapore in the context of global health. Singapore is therefore perceived as an attractive location for research due to its advances in technology, infrastructure, and expertise.

Some participants also attributed Singapore's success to the supportive role of the government in academia. The positive working relationship between policy-makers and academics was perceived to have advanced various research agendas in public health. As emphasized by a participant:

> *"We're trying to see how we can work together with academics to do research that can be translated into policies, into programs for policy makers to understand […] what kinds of research can be done, and to have a better working relationship with academics, and then for academics to understand also the standpoint of policy-makers […] I think in Singapore, we've been doing quite well."*
> *(Singapore, Government)*

*Health Outcomes and Access*

Apart from contributions in academia, some participants commented on Singapore's successes in terms of its progress in the achievements of the MDGs, particularly in healthcare. As described by a participant:

> *"[...] look at the MDGs, by the time it was pushed, places like Singapore had already achieved everything [...] There's so many interesting problems out there. Not in Singapore, mind you, especially around universal healthcare."*
> *(Singapore, Academia)*

*Good Governance*

For some participants, Singapore's success at achieving these global health goals is partly due to the political stability and good governance of the country relative to regional neighbors, who mostly remain in the process of political transition. As described by a participant:

> *"A lot of [Southeast Asian countries] go up and falter because of institutional structures like governance, corruption and all that, so the sequencing is that, if you've not successfully transitioned in having democratic institutions and even if you don't have full democracy. You have to have good governance and this is what Singapore is all about."*
> *(Singapore, Academia)*

***Hesitation to Play a Greater Role in Global Health***

*Singapore's Priorities*

Many participants spoke of how Singapore's economic pragmatism has, over time, shaped its priorities in policy-making within the country and beyond. Some participants explained that Singapore's global health focus was on pandemic preparedness and combatting infectious diseases, due to the potential threats to national security and economic stability. A participant describes:

> *"When you look at infectious diseases and security issues, that's the one that push the [Singapore] government to set up all these task forces and all that. That's the reality, either you provide the incentive, or there's money to be made, or you threaten the stability, or where people will lose money, then they will act."*
> *(Singapore, Academia)*

Nonetheless, participants also highlighted that the focus on economic development is not unique to Singapore but evident across the region, where a country's standing is measured by its economic growth. Consequently, Singapore and its neighbours face tensions between competing priorities in health and other sectors including trade and infrastructure, as exemplified below:

> *"The mantra in this part of the world has been economic development. Everything is measured in terms of percentage GDP growth […] I think the political powers [...] realize that you can't have good GDP growth, economic*

*asked to invest in it, it is like less of a priority than investing in a new port, or more communications infrastructure, or better roads, or train lanes."*
*(Singapore, Academia)*

Despite the recognition that health is a 'public good' and that protecting priorities in health is ultimately an investment in the country's future and wealth, participants shared that the challenge remains for Singapore to put this in practice in the global health context. As described by one participant, an example that illustrates this point is Singapore's response to the transboundary issue of severe haze originating from Indonesia:

*"When you look at a country like Malaysia and Singapore, even though they are actually at the receiving end of the health impact of haze, [they] actually took a very very long time to do something about it because the practitioners in Indonesia are owned by a lot of Singaporean and Malaysian interests."*
*(Global, UN Agency)*

In addition to the pragmatism that is perceived to have shaped its priorities thus far, several participants also described Singapore as focused primarily on being self-sufficient as a country, paying primary attention to ensuring that local needs are first and foremost met. Nonetheless, many participants noted a pervasive lack of inclusiveness for non-citizens within healthcare systems across the region, despite the extensive mobility of migrant workers within Southeast Asia. A participant elaborated:

*"We are encouraging people in ASEAN to be more mobile, to reap the economic benefits of mobility, but we are not ready to provide health care needs of non-citizens."*
*(Philippines, Regional NGO)*

*Difficulties Contributing to Global Health Development*

Some participants felt that it is difficult for Singapore to contribute resources into regional global health development, and several reasons contributed to this. Firstly, as alluded to above, the existing focus of health care planning and policy remains focused on domestic issues, which is a phenomenon that occurs across Southeast Asia. The participant explains:

*"[...] what are the governments doing for public health? Most will only look domestically, and that's the same problem with Singapore."*
*(Singapore, Academia)*

Secondly, it is perceived that in the context of global health development, richer countries like Singapore may at times bear the brunt of the economic burden, but realize few gains. For instance, when it comes to resources for migrant health (which is significantly linked to global health in this region), the more developed

nations in Southeast Asia believe they bear disproportionate costs. A participant commented:

> *"Addressing migrant health in ASEAN [...] has been on the agenda, has been discussed, but […] the sticking point is in ASEAN, it needs to be like consensus. You know, you have disagreements among the states, and so, countries like Myanmar, Laos, or Vietnam, sending countries, were like, 'Yes, everyone should have, you know, migrant health inclusion be granted.', but then Singapore, Thailand and Malaysia are like, 'But we're the ones who have to pay for it.' "*
> *(Myanmar, UN Agency)*

Additionally, some participants admitted that Singapore's self-sufficiency and strong healthcare system has never placed it on the receiving end of global health development aid/support. A participant remarked:

> *"Singapore's never been a major recipient. They have always had the attitude that 'we can take care of ourselves', and by and large, they can. Very capable people in this country."*
> *(Singapore, Academia)*

***Perceptions of Singapore's Potential Role in Global Health***

*Greater Expectations of Singapore Despite Its Successes*

A common theme that emerged among participant narratives was having higher expectations of Singapore to do even more in global health. As demonstrated in this quote:

> *"People would say okay, so this is the Tiger economies and can't we be doing more for health?"*
> *[Myanmar, Local NGO]*

Notwithstanding Singapore's efforts thus far, many participants believed that Singapore has the financial resources to contribute to global health in a greater capacity. Several participants praised Singapore for taking a proactive role in providing humanitarian assistance in response to natural disasters in the region. Similarly, many spoke of the country's laudable efforts in global health security, particularly in pandemic preparedness. As described by a participant:

> *"I was there before the US launched the Global Health Security Agenda. But [Singapore] were already doing a lot of work before that, so they were already very strong on health security. In fact, the things they were doing were already shaping towards the Global Health Security Agenda."*
> *(Singapore, Government)*

However, despite this past and present involvement, some participants felt that Singapore could take on a greater leadership role within the development sector beyond humanitarian aid, and provide greater support in other areas including health systems strengthening, as explained by a participant:

> *"Singapore's leadership in these kind of areas is very much lacking. During the tsunami in Aceh, Singapore was the first country to send humanitarian aid through the armed forces, but in terms of other things, like building capacity, strengthening healthcare delivery systems, it's nowhere, nowhere to be seen. It's about time Singapore establishes an International Development Agency. You are so rich, you've got so much skill, you've got so much capacity within Singapore to help the region."*
> *(Singapore, Academia)*

Many participants pointed out that the success of Singapore's healthcare system is partly due to the substantial in-flow of skilled healthcare professionals from the region. Some participants raised concerns over the possible impact this might have on sending countries, as elaborated by two participants who agreed in a group interview:

> *"We are a little bit concerned about the reverse flow of competent individuals. You know, very competent [Myanmar healthcare workers], they will go and work in Singapore, for example, and then we get less qualified individuals coming and stationed in our hospitals."*
> *(Myanmar, Private Consultant)*

There is an implicit expectation for Singapore to contribute more, partly to make up for the loss that sending countries experience due to the brain drain of competent individuals who have played a role in Singapore's successes in healthcare provision.

*Singapore Could Further Increase Its Role in Academia*

Several interviewees spoke about harnessing Singapore's distinguished academic infrastructure and expertise to increase its contribution to global health, and possibly for Singaporean universities to take a larger leadership role in the region within the academic sector. A participant explained:

> *"[...] about leadership for global health, I think there is a role to play for universities and such institutions […] there is actually a need for [Singaporean] universities to show more leadership."*
> *(Global, UN Agency)*

Participants were hopeful that platforms such as the "Raffles Dialogue", which aims to bring key thinkers together to discuss future directions and challenges of

human well-being and health security, would encourage academic institutions in Singapore to contribute more actively in global health. A participant elaborates:

> *"[...] if the idea of the Raffles Dialogue develops in a way that it becomes established as 'the' event [...] that can then become the catalyst for the formation of [...] a Centre, or an Institute […] for Global health in the context of Asia. So you now, [are] showing, developing an idea, saying that we developed a network that will be doing top-quality research in collaboration with countries in the region."*
> *(Singapore, Academia)*

*Singapore Can Leverage Its Expertise to Seed Larger Projects*

Many interviewees considered how Singapore could contribute to global health in the region other than through its academic footprint, including innovative methods to contribute on a regional scale in spite of Singapore's comparatively limited size and resources in terms of quantity. A participant expressed hope that what Singapore lacked in quantity could be made up in quality, elaborating that:

> *"Singapore as a little red dot cannot fund all of the Indonesian system, but we can show in a little pilot through WHO […] and say, we are a WHO collaborating center, WHO has also endorsed us to provide some of this training, or research. That's the way we should function."*
> *(Singapore, Academia)*

Overall, it was perceived that Singapore can use its strengths in medical expertise, technology, and governance to develop targeted interventions which could be expressly designed for scale-up by larger entities including other governments, donors or regional agencies.

*Filling the Health Gap in ASEAN*

Singapore's involvement regionally was discussed in several interviews, particularly relative to ASEAN. Many interviewees pointed out that ASEAN faces a gap in integrating health regionally. For instance, a participant spoke about the existence of the architecture, but not the expertise, for ASEAN to do more for health.

> *"The role of ASEAN, you look at some of their agreements and all, [health is] supposed to be all there. But the […] truth is does it work in practice, you see? So while we are very hopeful. Like you know, ASEAN will fill in the gaps that WHO cannot for whatever historical reason, and having done consultancies for both, I'll tell you actually, we're not there. The expertise is not there."*
> *(Singapore, Academia)*

Supporting this, another participant explained that ASEAN's small budget poses difficulties in contributing to the regional health landscape:

> *"[...] a part of the problem why the ASEAN Secretariat is weak technically, in the health field, is because they have a very small budget. Someone told me that they had a budget only like less than 10 million dollars a year."*
> *(Singapore, Academia)*

Participants also talked about the lack of a "health community" in SEA as compared to other parts of the world. Given the constraints on ASEAN and its potential to contribute significantly to global health, some interviewees expressed the need for a country to take a leadership role within ASEAN to encourage further engagement. A participant elaborates:

> *"I think the ten countries are at very different levels and are prioritizing things that are very different [...] I think it would be quite a challenge to actually get them all together to look at global health but I think maybe at the very top level, central level, there just needs to be a really good champion that comes on-board. I would say ASEAN would be a good platform to do that but then you will just need very strong political will to do it."*
> *(Cambodia, International NGO)*

### *Perceived Benefits if Singapore Increases Its Role in Global Health and Its Willingness to Do So*

*Practical benefits to increasing its role*

Respondents suggested a range of practical reasons for Singapore to increase its role, given its current focus on domestic health. Some reasons were related to diplomacy, with some participants making the point that global health works as soft power for Singapore, while others suggested that global health could be a stepping stone to solving other difficult transnational issues:

> *"In terms of the migration issue that maybe health could be the entry point to solve all these other issues; you know political, economic, confronting mobility etc."*
> *(Philippines, Regional NGO)*

Another practical reason for increasing Singapore's role in global health is the necessity for Singapore to have a regional focus in health due to its unique status as a small country dependent on regional cooperation.

> *"We have to also put the global health training within [Singapore]. We're not just training for domestic work, you know. We're training you for international work where you end up going to Africa and all that [...] we're very very practical, end up doing work in the region. Cause no man is an island.*

*Singapore is not a fortress. You have to. So my focus has always been regional, and you have to teach that well, that the Singaporean future public health practitioner has to have a regional focus."*
*(Singapore, Academia)*

Finally, some participants pointed out that much of what determines health is beyond the health system. Thus, having Singapore's health workforce look outside their own sector and country would work to Singapore's benefit.

*"[…] if you are actually coming from the social determinants of health perspective, you know that there are estimates like 80% of the health and well-being of populations are actually shaped by sectors beyond ours. [...] so we need to talk to other sectors more, but very few are doing that. Perhaps very few are capable of doing that. Doctors are not trained to be diplomats or negotiators with other sectors. We are taught about how to communicate with patients. We are not taught to talk to mayors, or governors, or presidents, or ministers of energy or labor. So, I think that is why, the health community should embrace that additional responsibility in the spirit of the Health In All Policy approach, HIAP, in order to foster global health cooperation across sectors across disciplines."*
*(Philippines, Regional NGO)*

*Perceptions on Singapore's Willingness to Increase Its Role*

While respondents perceived benefits from an increased Singapore role, perceptions of Singapore's willingness to do so were mixed. Some participants saw Singapore as ready to take up the mantle of global health leadership, as described by this participant:

*"My understanding is that Singapore is now turning outward from a very long time of looking inward as well. So while we don't have a cooperation strategy with Singapore, from everything I can tell, Singapore is now wanting to do the same [...] taking global stage,"*
*(Regional, UN Agency)*

Some participants felt that Singapore has the required mechanisms to contribute to global health but lacks the political will to realign its priorities and pragmatism. One participant explains:

*"[...] it's very difficult to explain to taxpayers that, 'Oh, you know, we are funding money to more research that is based in other countries.' I think people still don't understand why they must do that [...] but if you can kind of latch on, like, implement [...] big data [...] to let them understand the link towards global health and how it affects them, I think it will be more acceptable. When it's more acceptable by the public, somehow there will be better political will and then things will move."*

*(Cambodia, International NGO)*

Nonetheless, there is a general sentiment among participants that once Singapore decides to play a larger role and invest in an area of interest like global health, it will be done well given Singapore's excellent infrastructure and availability of resources. A participant asserted:

> *"I think the thing about Singapore is that I think once it has decided on the path and how to do it, [Singapore] will get it done."*
> *(Cambodia, International NGO)*

## DISCUSSION

This study explored perceptions of Singapore's role in global health among stakeholders across SEA. Findings suggest that Singapore is perceived as successful in achieving its MDGs, its progress in healthcare, and its ability to exercise good governance. Nevertheless, several obstacles were cited as hampering Singapore's willingness and ability to do more for global health. Many perceived that Singapore prioritises the health, economic prosperity and security of Singaporeans and empathised with the predicaments Singapore faces in global health development. Ways proposed for Singapore to increase its global health role involved leveraging its well-established academic institutions, good governance structures, and utilising ASEAN as a platform for global health engagement.

Stuckler and Mckee (2008) proposed five metaphors which represents the possible policy making priorities that countries such as Singapore can consider in developing their global health policy (Table 3). As mentioned above, Jahncke at al (2010) suggested that Singapore could benefit from contributions in global health through the application of the five metaphors.

These metaphors were postulated to understand the various strategies that may be adopted within the global health policy-making process. For example, global health strategies that target universal goals, such as funding immunization programmes in a neighbouring country, can accomplish multiple goals simultaneously. This includes protecting Singapore's health security, improving public health, and bolstering Singapore's reputation and diplomatic relations abroad. These metaphors are largely interlinked and serve as a useful heuristic to guide global health policy adoption. Considering the complexity of the local and global health architecture within Singapore, these five metaphors enable an understanding of which strategies may be of greatest priority to Singapore and which areas Singapore may consider further advancing. As such, the findings will be analysed through the lens of these five metaphors.

**Table 3: Five Metaphors of Global Health Policy**

| *Principle* | *Example Goals* | *Example Institutions* |
|---|---|---|
| Global health as security | Protect against bioterror, antibiotic resistance, pandemic preparedness etc. | Ministry of Defense, Communicable Disease Centre, Ministry of Health |
| Global health as investment | Enhance economic development through the promotion of health | Economic Development Board, Ministry of Health |
| Global Health as foreign policy | Promote trade, alliances, and cooperation | Singapore International Foundation, Ministry of Foreign Affairs |
| Global health as charity | Reduce poverty with a focus on the most vulnerable | Singapore Red Cross, Mercy Relief |
| Global health as public health | Reduce the global burden of disease | Ministry of Health, Academic institutions |

(Adapted from Stuckler and Mckee 2008)

The first metaphor is global health as 'security'. In conceptualizing global health security, WHO warned against allowing a narrow focus on national health security to override commitments to global health (Flahault et al. 2016), as observed during the world's response to the Ebola epidemic (Heymann et al. 2015). Our findings point to Singapore being motivated to engage in global health when the country's health security is under threat, for instance during the SARS outbreak when thousands of people were quarantined (Tan 2006) and billions of dollars were lost, compromising the country's economic growth (Keogh-Brown et al. 2008). In our study, pandemic preparedness was perceived as a primary impetus for Singapore to work towards greater regional and global engagement in health. Gushulak and colleagues (2010) emphasized in a literature review that the 'globalisation of health risks' in a changing migration landscape due to increased mobility can pose infectious disease threats to nations such as Singapore where mobility is high. Our findings imply that Singapore's approach to ensuring global health security should look beyond pandemic preparedness to other strategies, such as health system strengthening in the region, to be fully secure against infectious disease threats. Some respondents believe that Singapore has already taken steps towards this by participating in the US-led 2014 Global Health Security Agenda.

Our findings also indicate that Singapore's government could be induced to do more by looking at global health as 'investment'. Singapore's extensive investments in health domestically are perceived to have contributed to the growing industry of medical tourism in the country. Although medical tourism benefits the region's elites who can afford it (Pocock and Phua 2011), our participants remained critical of Singapore's limited contribution in global health beyond this group. Participants were

sympathetic towards the perception that rich countries like Singapore commonly shoulder the bulk of investments with few returns when it comes to global health. However, this perception may itself be inaccurate: in a study exploring the UK's footprint on health globally, the UK was described to have benefitted from the promotion of life sciences and health industries, improvements in cross-sectoral synergies, increased investments in health, and the draw-in of the best talent (Hasan et al. 2015). The report also showed that the return on investments extended beyond the realm of health, such as in the economic growth and goodwill gained across borders (Herrick 2017). This demonstrates that there is significant value in contributing to global health, even for rich nations like the UK.

The idea of global health as beneficial for 'foreign policy' also surfaced in the findings. The interplay between politics, foreign policy, and global health policy has given rise to the field of global health diplomacy (Ruckert et al. 2016). In fact, the value of global health in terms of advancing foreign policy goals has been acknowledged with formal government bodies dedicated to this purpose in the US, UK, and EU (Kevany 2014). Some respondents shared this view and saw engaging in global health as a means to enhance Singapore's soft power. Other respondents suggested that moving towards more regional cooperation in health could also benefit Singapore in establishing cooperation in non-health related issues such as the rights of migrants. Respondents pinpointed one such political consideration - a tendency among ASEAN governments to value trade over health in their foreign policy. Nevertheless, taking a global health perspective can help governments better manage tradeoffs between health and trade in their foreign policy. Thailand, for example, has successfully integrated health with trade policies by purposefully facilitating the understanding of trade effects on health at the individual level, establishing mechanisms and networks to enhance health interests and advocate for health within trade negotiations, and building capacity of health officials to deal with trade-related health issues (Thaiprayoon and Smith 2015). Singapore may benefit from taking a similar view.

The remaining two metaphors for global health policy relate to 'charity' and 'public health'. According to Stuckler and Mckee (2008), promotion of global health as a form of charity focuses on alleviating poverty with an emphasis on reaching the most vulnerable. Singapore is perceived to have adopted a commendable role in global health through the years of humanitarian assistance rendered to its neighbors in times of natural disasters. In recent years, however, the discourse on global health aid has evolved to focus on fostering synergies between vertical and horizontal programs, with an emphasis on health systems strengthening (Balabanova et al. 2010). In line with this, developed countries such as Japan have aligned their priorities in development aid towards strengthening the health systems of developing countries (Yuasa 2013). Similarly, our findings suggest that Singapore could support less developed nations in global health, given its successes and expertise in health systems and its fiscal viability. This is consistent with previous proposals for the establishment of funding mechanisms for global health research and development in health systems strengthening for Singapore (Jahncke et al. 2010).

Lastly, conceiving global health as 'public health' constitutes an investment in maximizing the health of all human beings and reducing the global burden of disease (Mckee et al. 2008). Ultimately, health in the global context should be perceived as a shared responsibility among all stakeholders and a collective response is necessary to align efforts towards achieving global health goals (Gostin et al. 2010, Otterson et al. 2014). Our findings validate the results of previous global health reports (Lim et al. 2016, Barber et al. 2017), in that Singapore is widely held to be a leading success in its progress in healthcare and achievements in global health goals, such as the MDGs. While much of this success is perceived as motivated by pragmatic priorities, it serves as a good example to illustrate the link between state investment in global health issues and public health benefits at the local level. Fundamentally, nation states have a responsibility to protect and maintain the health of their population; however, as a result of rapid globalization, various determinants of health are inherently global demanding all states to take action in global health governance (Otterson et al. 2014). This requires states to engage and collaborate with each other, such as building up big data capacities to aid global health planning amongst and within states (Wyber et al. 2015). Singapore could potentially reap significant benefits from such engagement with the global health community.

### *Future Research and Opportunities for Agenda Setting*

These findings provide some direction on priorities for future research, facilitating agenda-setting for global health in Singapore. Drawing on these findings and the pioneering work of Jahncke et al. (2010), a more comprehensive study pertaining to Singapore's contributions and impact on global health in various sectors could be beneficial. In recent years, the UK has conducted such research on mapping out its contribution to global health in different sectors (Hasan et al. 2015) (Table 4).

The evidence generated allowed the UK to strengthen its influence in the health sector and lead the way on improving global health (Hasan et al. 2015). While our study's findings provide valuable insight on Singapore's active contribution in certain areas including the state and academic sector, the overall study lacks the comprehensiveness of the UK report. As propounded by Jahncke et al. (2010), multi-sectoral and multidisciplinary partnerships are fundamental to the development of global health efforts and initiatives. As such, we suggest that Singapore conduct a similar comprehensive study to explore its role in global health and how it can contribute further through the various sectors. The evidence gathered can then be presented to policymakers and stakeholders in Singapore through the medium of a policy dialogue to facilitate strategic planning processes in relation to global health. A multi-sectoral approach incorporating expertise from fields such as international relations will be needed to address any possible political sensitivities that may arise. Fields such as economics will be crucial in demonstrating the cost effectiveness of potentially investing in global health. Overall, such a study will serve as a useful basis for Singapore to strengthen its position as a global health leader. It will also provide insights on how regional actors perceive Singapore's role in global health, thus enabling SEA countries to examine their own role in global health and how they may

converge regionally to embrace the "complex interdependence" global health requires (Frenk et al., 2014).

**Table 4: Sectors mapped out to understand UK's role in global health**

| Sector as in UK report | Groups concerned | Explanation |
|---|---|---|
| State | All areas of government, ministries and statutory boards funded by public money. | Improving global health through state policies and leadership on global health, working domestically to improve health overseas, creating an enabling environment for other sectors engaged in global health to thrive.<br><br>Eg. National health service training healthcare professionals from abroad. |
| Academic | Actors who fund and conduct health research globally in various fields, for example, Biological sciences, economics and public health. | Improving global health through trainings of health professionals, providing sufficient funding for research which transcend national borders, research collaborations between university and institutes and disseminating key research through renowned journals.<br><br>Eg, The funding from the Wellcome Trust in the UK |
| Commercial | Actors in the "for-profit" sector selling goods and services who either contribute to the health system in some way. | Improving global health through the export of goods and services which further health globally<br><br>Eg. Healthcare consultancies. |
| Non-Governmental Organisation | Actors outside of the state who work on a "non-profit" basis to improve health globally. | Improving global health through the delivery of health services, capacity building, advocacy and research globally through the spheres of international development or humanitarian action.<br><br>Eg. Disaster assistance through the Disasters Emergency Committee. |

(Adapted from Hasan et al. 2015)

### *Strengths and Limitations*

To our knowledge, this is the first qualitative study exploring key stakeholders' perspectives on Singapore's role and contribution to health globally. A strength of this paper is that we conducted in-depth interviews with a wide range of actors involved in global health (i.e. government, UN agencies, civil society, donors, academia, and the private sector) and from a variety of geographical locations (i.e. Singapore, the Philippines, Cambodia, Myanmar, India and Thailand). There are three main limitations to this study. Firstly, the qualitative data for this paper was drawn from a larger study exploring the global health architecture in SEA. Information on Singapore's role and contributions in global health was not purposefully elicited for every interview unless brought up by the participant. As a result, the issues discussed on Singapore differed across participants. Secondly, we looked only at the narratives of participants who had knowledge or opinions about Singapore's role in global health; hence, findings may not be representative of the entire global health sector in SEA. Thirdly, while participants were from a wide array of organizations and countries, the majority have primary expertise in health. Considering the inter-sectoral nature of global health as a discipline, our data may be lacking in richness.

## CONCLUSION

This study provides insight on Singapore's role and contributions in global health as perceived by stakeholders in health across Southeast Asia. Overall, Singapore is recognized for its accomplishments in health globally and the quality of its academic institutions. Participants viewed Singapore's current role and contributions as positive, but with great unrealized potential. The country's pragmatism in setting health priorities is perceived as an obstacle in committing further to global health, which is regarded as an act that occurs at the expense of Singapore. Notwithstanding, our findings suggest that contributions in global health in fact represent valuable opportunities for Singapore in bolstering its security, economy, and foreign relations, while fulfilling more charitable goals and contributing to a reduction in the global disease burden. Overall, this paper elucidates that there are many practical benefits for Singapore should it fulfill its potential roles in global health. Hence, for further strategic planning, there is a need for more comprehensive and multi-sectoral research on Singapore's existing global health footprint and its potential to contribute further in global health.

## REFERENCES


Balabanova, Dina, Martin McKee, Anne Mills, Gill Walt, and Andy Haines, "What Can Global Health Institutions Do to Help Strengthen Health Systems in Low Income Countries?" *Health Research Policy and Systems* 8 (2010): 22. doi:10.1186/1478-4505-8-22.

Barber, Ryan M, Nancy Fullman, Reed J D Sorensen, Thomas Bollyky, Martin McKee, Ellen Nolte, Amanuel Alemu Abajobir, et al., "Healthcare Access and Quality Index Based on Mortality from Causes Amenable to Personal Health Care in 195 Countries and Territories, 1990–2015: A Novel Analysis from the Global Burden of Disease Study 2015." *The Lancet* 390(2017): 231-266. doi:10.1016/S0140-6736(17)30818-8.

Chongsuvivatwong, Virasakdi, Kai Hong Phua, Mui Teng Yap, Nicola S. Pocock, Jamal H. Hashim, Rethy Chhem, Siswanto Agus Wilopo, and Alan D. Lopez, "Health and Health-Care Systems in Southeast Asia: Diversity and Transitions." *The Lancet* 377 (2011): 429–437.

Flahault, Antoine, Didier Wernli, Patrick Zylberman, and Marcel Tanner, "From Global Health Security to Global Health Solidarity, Security and Sustainability." *Bulletin of the World Health Organization* 94 (2016): 863–863. doi:10.2471/BLT.16.171488.

Frenk, Julio, Octavio Gómez-Dantés, and Suerie Moon, "From Sovereignty to Solidarity: A Renewed Concept of Global Health for an Era of Complex Interdependence." *The Lancet* 383 (2014): 94–97.

Gostin, Lawrence O, Mark Heywood, Gorik Ooms, Anand Grover, John-Arne Røttingen, and Wang Chenguang, "National and Global Responsibilities for Health." *Bulletin of the World Health Organization* 88 (2010): 719–719A. doi:10.2471/BLT.10.082636.

Gushulak, BD, J Weekers, and DW MacPherson, "Migrants and Emerging Public Health Issues in a Globalized World: Threats, Risks and Challenges, an Evidence-Based Framework." *Emerging Health Threats Journal* 2 (2010). doi:10.3134/ehtj.09.010.

Hasan, Nadeem, Sarah Curran, Arnoupe Jhass, Shoba Poduval, and Helena Legido-Quigley, "The UK's Contribution to Health Globally.", *All-Party Parliamentary Group, United Kingdom,* 2015, http://www.appgglobalhealth.org.uk/download/i/mark_dl/u/4009611296/4622063799/The%20UK%E2%80%99s%20contribution%20to%20health%20globally_FULL.pdf. (Last Accessed 8th August 2017)

Heymann, David L, Lincoln Chen, Keizo Takemi, David P Fidler, Jordan W Tappero, Mathew J Thomas, Thomas A Kenyon, et al, "Global Health Security: The Wider Lessons from the West African Ebola Virus Disease Epidemic." *The Lancet* 385 (2015): 1884–1901. doi:10.1016/S0140-6736(15)60858-3.

Hoffman, Steven J, Clarke B Cole, Mark Pearcey, "Mapping Global Health Architecture to Inform the Future", *Chatham House, The Royal Institute of International Affairs*, 2015

http://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20150120GlobalHealthArchitectureHoffmanColePearceyUpdate.pdf. (Last Accessed 8th August 2017)

Jahncke, E., M. K. Lim, A. Seow, K. S. Chia and A. Wilder-Smith, "Global Health: Challenges and Opportunities for Singapore." *Singapore Medical Journal* 51 (2010): 536–541.

Keogh-Brown, Marcus Richard, and Richard David Smith, "The Economic Impact of SARS: How Does the Reality Match the Predictions?" *Health Policy* 88 (2008): 110–20. doi:10.1016/j.healthpol.2008.03.003.

Kevany, Sebastian, "Global Health Diplomacy: A 'Deus Ex Machina' for International Development and Relations." *International Journal of Health Policy and Management* 3 (2014): 111–12. doi:10.15171/ijhpm.2014.67.

Lamy, Marie, and Kai Hong Phua, "Southeast Asian Cooperation in Health: A Comparative Perspective on Regional Health Governance in ASEAN and the EU." *Asia Europe Journal* 10 (2012): 233–50. doi:10.1007/s10308-012-0335-1.

Lim, Stephen S., Kate Allen, Zulfiqar A. Bhutta, Lalit Dandona, Mohammad H. Forouzanfar, Nancy Fullman, and Peter W. Gething, "Measuring the Health-Related Sustainable Development Goals in 188 Countries: A Baseline Analysis from the Global Burden of Disease Study 2015." *The Lancet* 388 (2016): 1813–50. doi:10.1016/S0140-6736(16)31467-2.

Moon, Suerie, Devi Sridhar, Muhammad A. Pate, Ashish K. Jha, Chelsea Clinton, Sophie Delaunay, and Valnora Edwin, "Will Ebola Change the Game? Ten Essential Reforms before the next Pandemic. The Report of the Harvard-LSHTM Independent Panel on the Global Response to Ebola." *The Lancet* 386 (2015): 2204–21. doi:10.1016/S0140-6736(15)00946-0.

Ottersen, Ole Petter, Jashodhara Dasgupta, Chantal Blouin, Paulo Buss, Virasakdi Chongsuvivatwong, Julio Frenk, and Sakiko Fukuda-Parr "The Political Origins of Health Inequity: Prospects for Change." *The Lancet* 383 (2014): 630–67. doi:10.1016/S0140-6736(13)62407-1.

Pocock, Nicola S., and Kai Hong Phua, "Medical Tourism and Policy Implications for Health Systems: A Conceptual Framework from a Comparative Study of Thailand, Singapore and Malaysia." *Globalization and Health* 7 (2011): 12. doi:10.1186/1744-8603-7-12.

Ruckert, Arne, Ronald Labont, Raphael Lencucha, Vivien Runnels, and Michelle Gagnon, "Global Health Diplomacy: A Critical Review of the Literature." *Social Science & Medicine* 155 April (2016): 61–72. doi:10.1016/j.socscimed.2016.03.004.

Stuckler, David, and Martin McKee, "Five Metaphors about Global-Health Policy." *The Lancet* 372 (2008): 95–97. doi:10.1016/S0140-6736(08)61013-2.

Tan, Chorh-Chuan, "SARS in Singapore-Key Lessons from an Epidemic." *Annals-Academy of Medicine Singapore* 35 (2006): 345-49.

Tan, Yeling, Kelley Lee, and Tikki Pang, "Global Health Governance and the Rise of Asia: Global Health Governance and the Rise of Asia." *Global Policy* 3 (2012): 324–35. doi:10.1111/j.1758-5899.2012.00177.x.

Thaiprayoon, Suriwan, and Richard Smith, "Capacity Building for Global Health Diplomacy: Thailand's Experience of Trade and Health." *Health Policy and Planning* 30 (2015): 1118–28. doi:10.1093/heapol/czu117.

United Nations Development Programme, "Overview: Human Development Report 2016.", *United Nations Development Programme* , 2016, http:/http://hdr.undp.org/sites/default/files/HDR2016_EN_Overview_Web.pdf/books.google.com/books?hl=en&lr=&id=Ia4l7gkgbIsC&oi=fnd&pg=PR8&dq=%22rights+reserved.+No+part+of+this+publication+may+be+reproduced,+stored+in+a+retrieval+system+or+transmitted,+in+any+form+or+by+means,%22+%22Development+for%22+&ots=96KQgmmpl_&sig=OROoBoVO6k78bvHriUBIOxfENgg. (Last Accessed 8th August 2017)

United Nations Development Programme. "Sustainable Development Goals", accessed August 8, 2017, http://www.undp.org/content/undp/en/home/sustainable-development-goals.html

Van de Pas, Remco, Peter S. Hill, Rachel Hammonds, Gorik Ooms, Lisa Forman, Attiya Waris, Claire E. Brolan, Martin McKee, and Devi Sridhar, "Global Health Governance in the Sustainable Development Goals: Is It Grounded in the Right to Health?" *Global Challenges* 1 (2017): 47–60. doi:10.1002/gch2.1022.

Wyber, Rosemary, Samuel Vaillancourt, William Perry, Priya Mannava, Temitope Folaranmi, and Leo Anthony Celi, "Big data in global health: improving health in low-and middle-income countries." *Bulletin of the World Health Organization* 93, no. 3 (2015): 203-208.

World Bank. "World Bank Country and Lending Groups – World Bank Data Help Desk", accessed August 8, 2017, https://datahelpdesk.worldbank.org/knowledgebase/articles/906519-world-bank-country-and-lending-groups

RESEARCH ARTICLE

# Protecting the Vertical Space of Cities: Perspectives for Singapore

***Muhammad Faizal Bin Abdul Rahman*** [1]

**Keywords**: Vertical urbanism, vertical cities, homeland security, drones, building internet of things

**Suggested Article Citation**: Muhammad, Faizal. 2017. "Protecting the Vertical Space of Cities: Perspectives for Singapore" *Asian Journal of Public Affairs* 10(1): p.27-51

http://dx.doi.org/10.18003/ajpa.20179

ISSN 1793-5342 (print); ISSN 2382-6134 (online), 

**ABSTRACT**

*Singapore and other global cities are increasingly exploring the vertical space – vertical urbanism - to address challenges from land scarcity and growing urbanisation. As urbanisation can shape the nature of crime and security threats, there would be a need for vertical urbanism to be an essential consideration in the forward planning for vertical policing strategies by homeland security agencies. While threats to high-rise buildings are not new, vertical urbanism is changing the environment even as it optimises space utilisation (including lower airspace) and this may plausibly expand the attack surface of cities by presenting additional vectors for threats. Existing regulatory frameworks and policies, and operational procedures need to adapt to address the plausible threats that may ascend amid the social and economic vibrancy of the vertical space of future cities. Currently, such frameworks generally look into drone regulations and high-rise building security as separate domains rather than subsets of the vertical space. This paper employs a documentary approach to envision the vertical space and its security dimension, plausible vertical security challenges and concludes with a specific policy recommendation that may be helpful to cities including Singapore.*

[1] Muhammad Faizal (ismfaizal@ntu.edu.sg) is a Research Fellow with the Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies (RSIS). He formerly served in the Singapore Ministry of Home Affairs including in the National Security Coordination Secretariat and the Singapore Police Force.

## INTRODUCTION

Singapore and other global cities are increasingly exploring the vertical space as a sustainable and smart approach – improving public services by integrating traditional city infrastructure with digital technologies (Dlodlo 2016) - to address physical challenges that arise from growing urbanisation, population growth and land constraints. It is set to become more automated and crowded in the foreseeable future (National League of Cities 2016, p. 25).

With innovation in architectural ideas and advances in smart technologies, the vertical space of cities including Singapore's can be territorialised to accommodate a larger population, social and economic activities. Specifically, on territorialisation, regulatory policies and systems that would be put in place to ensure order would need to clearly define the different zones in the vertical space as public, semi-public/semi-private, and private. Stakeholders (public and private) of the vertical space would have to exercise a sense of ownership and responsibility over their respective zones, and this would over time lead to the formation and enforcement of accepted norms and behaviour in the vertical space (Townsley et al. 2013, p. 20).

Stakeholders would come from the proliferation of vertical communities as buildings and infrastructure become more high-rise, more mixed-use and smart; and enhanced connectivity as more public transport and mobility infrastructure are built vertically. The lower (low altitude) airspace may be the streets of the future with improvements in technology and regulations on the use of drones for consumer and commercial activities. The lower airspace – publicly navigable for drones – currently differs in the definition (height limit of 200 – 500 feet above ground) across countries and terrain (urban or non-urban) as it is based on localised considerations such as safety, privacy and commerce (Lim 2015). Nonetheless, it will in the future comprise a network of carefully defined aerial lanes and zones that characterise the drone traffic management systems that several cities are developing (Low, Gan and Mao 2014).

Such developments – vertical urbanism - would have strategic implications on homeland security for cities including Singapore specifically in the domains of law enforcement, public order and counter-terrorism.

Given the complexity in policing the vertical space, there would be a growing need to examine the security dimension in the vertical aspects of cities and urban life, especially as existing studies done in this research area are few. For Singapore, the rise of this security dimension is presaged by some existing developments: the passing of the Unmanned Aircraft (Public Safety and Security) Act in 2015; the installation of high-rise Police CCTV surveillance (Hawk Eye) cameras on selected buildings in 2013; the unveiling of security drones during the Police Work-plan Seminar 2015; and deployment of Police National Service officers for "vertical policing" of high-rise residential buildings that began as early as 1979.

This qualitative study uses a documentary research that draws on the review of publicly available journals, industry reports and analysis of news articles. A caveat to this methodology, while it attempts to envision the future, is that the implications of vertical urbanism to the security of cities would become clearer only in the long term. Like scenario planning, projections are predicated on current perceptions of trends and driving forces and would evolve subject to the "rapidly changing and complex environment" (Public Service Division 2011, p. 13).

The paper will first examine the background of the vertical space as well as its security dimension in order to set the stage for discussion. The paper then continues with the exploration of plausible vertical security challenges. These include changes to the geography of the operating environment; and emergent threats (and challenges) possibly presenting deep policy implications by introducing additional vectors for hostile acts that can challenge the current capabilities of homeland security agencies (e.g. police and civil defence). The paper concludes by laying a vertical policing framework as a specific policy recommendation, comprising strategies in the areas of intelligence, frontline operations, planning and community vigilance that may be useful for Singapore.

## LITERATURE REVIEW

Vertical security has been defined in some articles as repurposing drones – originally a military capability – to extend police air (surveillance and search) power over the city which was achieved through the use of manned helicopters (Wall 2013; Adey 2010). Other articles refer to the "verticalisation" or provision of effective policing services to communities in high-density, high-rise cities that are expanding vertically (Benites 2008; Townsley et al. 2013). Several distinct developments in the recent years across the globe broadly reflect these definitions and would collectively characterise vertical security.

Given that drones are expected to be part of people's daily lives in the foreseeable future, the European Commission is developing a "U-Space" drone traffic management system comparable to the Unmanned Traffic Management (UTM) system that U.S is developing; these systems would incorporate law enforcement and security requirements (Carey 2017). Given the need to ensure the physical security and resilience of high-rise buildings (and people within) against crime and terrorist attacks, the U.S Homeland Security Department published the Reference Manual to Mitigate Potential Terrorist Attacks against Buildings (2nd Edition) in 2011. Cybersecurity is increasingly intertwined with building and infrastructure security due to the proliferation of smart devices and systems in them, and thus the U.S government, for example, is investing heavily into research in this area (Memoori 2017; Tankard 2015; DHS 2015). Given the need to improve emergency preparedness and social resilience in vertical communities, the City of Vancouver in Canada had projects that include organising "vertical block parties" to promote neighbourly relations (Chia 2014).

The definitions may change and coalesce as cities expand vertically, become more digitised, and more central to national security; they entail moving beyond the contemporary two-dimensional to a three-dimensional appreciation of the urban space as discussed in this paper (Graham and Hewitt 2012).

## BACKGROUND OF VERTICAL URBANISM

Growing urbanisation is characterised not only by increasing urban densities (buildings and populations) and urban footprint, but also the expansion of the vertical space. Global cities such as Singapore are increasingly exploring the use of the vertical space – vertical urbanism - as a smart and sustainable approach to address the complex challenges of accommodating growths in population and socio-economic activities amid land constraints. This approach is practicable given innovation in architectural ideas and advances in smart technologies, hence presaging the territorialisation of the vertical space of cities (Shaw 2017, p. 1).

Vertical urbanism, as argued in this paper, would primarily comprise of: (a) applying novel concepts for space utilisation such as broadening current concepts of land use zoning to build more (very) high-rise, mixed-use and smart buildings or infrastructure; and (b) vibrant lower airspace resulting from growth in consumer and commercial drone market. Essentially, the appreciation of vertical urbanism for policymaking including in homeland security needs to be framed through airspaces in which high-rise buildings are a subset (Harris 2015). Currently, regulatory frameworks and policies, and operational procedures generally look into drone regulations and high-rise building security as separate domains rather than subsets of the vertical space.

### *Vertical Cities*

First, high-rise high-density vertical cities are the solution to land scarcity (Wong 2004). Social, residential and commercial activities can develop in novel ways by spreading and happening in the vertical space as designed into buildings such as the Tanjong Pagar Centre and Pinnacle @ Duxton in Singapore, and Canaletto Tower in London. Such mixed-use buildings are also conceived as vertical neighbourhoods. Vertical communities are envisioned to proliferate as high-rise buildings and infrastructure can provide public amenities and draw more people at the upper levels, such as the Seoullo 2017 (1,024m long elevated park) in Seoul. Integrated road-rail viaducts such as the Tuas West Extension in Singapore can enhance transport connectivity while reducing road congestions. High-rise farms can be incorporated into residential and commercial buildings to help address food security issues and improve the efficiency of food supply chains for land scare cities (Teh 2016; Wee 2015).

Second, the global consumer and commercial drone market are expected to see strong growth in the foreseeable future (Forrest 2017). The lower airspace in cities can be envisioned to be the vertical streets of the future with improvements in

technology and regulations on the use of drones for a multitude of activities (Muhammad 2017a). For example, Singapore is exploring the use of drones for postal and delivery services (Hio 2017), and working towards developing a drone traffic management system for city airspace similar to ground road systems for automobiles (Hio 2016). Like in Dubai, Singapore may expand the use of drone technology to improve public transportation by possibly introducing autonomous flying taxis (e.g. EHang 184) in the foreseeable future (Soon 2017).

The scale of vertical cities may broaden as businesses, communities and governments discover more novel applications for (very) high-rise, mixed-use and smart buildings and infrastructure, and drone technology. This would be a natural and spatial evolution of cities that are embarking on "Smart Cities" initiatives to bring working and recreational spaces closer to living spaces while enhancing public amenities such as utilities, environment and transportation in a holistic manner (Calder 2017, p. 116).

Vertical urbanism would, however, have strategic implications on governance including in homeland security (law enforcement, public order and counterterrorism) as it essentially entails the vertical expansion of the public space. In policing the vertical space, security agencies would need to consider delineation between privately-owned and navigable lower airspace which may overlap with property ownership issues; circumstances where the aerial vantage point of drone traffic or high-rise activities could encroach into private space; enforcement of drone traffic; and smart building management (Muhammad 2017a; Widener 2016; Tankard 2015).

The complexities that vertical urbanism may pose on governance were encapsulated in an architectural website article "The Three-Dimensional City: How Drones Will Impact the Future Urban Landscape":

*"In the coming years, we may witness an increasing number of legal battles over the rights to airspace just as conflicts ensued with the emergence of automobiles at the time of the Model-T."*

*"But if drones become fixtures of our urban environment, what impact will they have on exterior spaces? And could they become as ubiquitous in our city's skies as cars on our streets?" (Rawn, 2015)*

New points and lines of vulnerabilities may arise and complicate law enforcement and emergency response efforts. For example, a municipal issue-related query (number 17) during one of Singapore's parliamentary session, asking about the security (drug activities, access and Police CCTVs) of then newly-introduced rooftop gardens in new residential estates, may have been a bellwether of emergent crime and security concerns in the vertical space (Twelfth Parliament of Singapore 2015, p. 267).

### *Vertical Security*

The vertical space of cities may over time be affected by emergent crime and security threats such as transnational crimes, public order issues, urban terrorism, and cyberattacks (by state and non-state actors) that currently and largely afflict the horizontal space of global cities. While threats to high-rise buildings are not new, vertical urbanism is changing the environment even as it optimises space utilisation (including lower airspace) and enhances urban livability. Thus, it may plausibly expand the attack surface of cities by presenting additional vectors – paths or means to gain access and create a malicious outcome - for both physical and cyber threats from criminals and terrorists. This stems from the inherent character of global cities as high-value targets given their growing strategic importance as the population and socio-economic centres of nation states, and drivers of the global economy (Dobbs et al. 2011).

Adversaries may over time find it increasingly viable to exploit the vertical space to target the people, supporting systems (places, technology and critical infrastructure) and iconic entities (buildings) that sustain modern urban life (Graham 2010, pp. 21, 266). Hence, security agencies would need to anticipate the plausible challenges, and develop policing strategies and capabilities to safeguard peace and order in the vertical space of cities.

There may be unexpected and unintended implications as similar to the horizontal space, for example, the vertical space may see conflicts as security agencies and adversaries vie for control (order vs. disorder). Furthermore, security measures such as vertical surveillance (e.g. police drones and high-rise Smart CCTVs) may shift the relationship between the people and security agencies as existing issues such as privacy and trust, and public expectations of police performance may find relevance in the vertical space (Graham 2016, pp. 13, 25).

Given the complexity in policing the vertical space, there is a growing need for strategic anticipation and analysis of the security dimension in the vertical aspects of cities and urban life, especially as existing studies done in this research area are few (Graham 2012, pp. 73 - 74).

## VERTICAL SECURITY CHALLENGES

### *Anticipate & Appreciate*

Homeland security agencies need to keep abreast of and analyse the various issues and trends that may shape the plausible scenarios of vertical urbanism in order to anticipate the emergent threats and challenges that may permeate the vertical space. The research should feed into the long-term strategic planning and capability development of agencies as these threats may have the potential to stretch their resources and challenge current operational procedures and tactics (Benites 2008, p. 8). There may also be deep policy implications in which security, social and economic issues may converge besides privacy and safety concerns.

A methodical appreciation of the terrain would be necessary as the inclusion of the vertical space into the operating landscape fundamentally expands and redefines the geography of cities by volume (three-dimensional) rather than by area (two-dimensional) (Dodge 2013). There would be implications on security functions such as police presence (patrols), community engagement, intelligence and surveillance, and incident response. For the vertical space to be safe and secure, these security functions must be able to oversee the lower airspace; assets and places in (very) high-rise, mixed-use and smart buildings or infrastructure; and the circulation of people and activities within (Adey 2010). The appreciation of the terrain in the vertical space would complement the research to anticipate and address the emergent threats, which this section will attempt to examine.

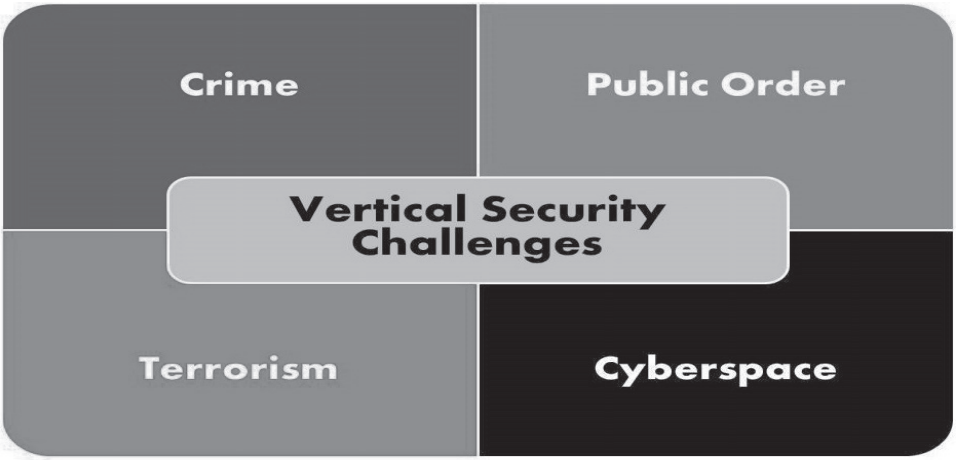
***Emergent Threats***

Underpinning these threats is the assumption that vertical urbanism may not fully protect people and assets from the "insecurities" or threats that exist in the horizontal space (Adey 2010). Rather, the threats may elevate and evolve into novel forms and its severity may be compounded by a false sense of security arising from high-rise living (Townsley et al. 2013, p. 78). An analogy would be how aerial accidents involving drones entail a novel (and vertical) form of traffic incidents that can harm people and property that are ordinarily shielded by height from the traffic incidents on the (horizontal) ground.

The elevation and evolution of threats would stem from the confluence of two factors that are intrinsic to vertical urbanism. First, the larger vertical (and public) space in (very) high-rise and mixed use buildings may act as "crime generators" that present more opportunities for perpetrators to relocate certain illicit activities or street crime in order to reduce the risk of police detection, or even widen their reach to seek more victims and ill-gotten gains (Townsley et al. 2013, p. 19). Second, the growing consumer and commercial drone market would result in the "colonisation" (by drones) of the vertical space and this is expected to present certain risks (e.g. misuse or device failure) that may proliferate (Crampton 2016, p. 143). Vertical space where the lower airspace and buildings may overlap due to indoor drone traffic may introduce a different set of threats (Ong 2016).

These emergent threats may unfold in the spheres of crime, public order, terrorism and cyberspace as shown in Figure 1, in which several scenarios are plausible.

**Figure 1: Spheres of Emergent Threats in the Vertical Space**




***Crime***

Criminals may be inspired by the proliferation of drones in increasingly high-rise cities to adapt and develop innovative tactics in order to commit various offences (e.g. burglary, robbery, sexual cases and unauthorised surveillance), and to evade detection by patrol robots and ubiquitous street-level police CCTVs. For example, drones may be used by criminals to facilitate breaking and entering of high-rise units (Browne 2017).

Drones may be used as delivery vehicles, for example, to peddle and deliver illicit or controlled items, thus circumventing existing laws and enforcement measures. Even today, criminals are known to leverage disruptive technologies such as drones and mobile-app enabled services in the commission of unlawful activities, and transforming the business models of criminal enterprises (Mogg 2017; Wong 2017).

Hence, vertical communities may experience vertical versions of crimes that were originally prevalent on the streets and low-rise buildings. Community-level crime prevention measures such as neighbourhood watch approaches such as "Crime Prevention through Environmental Design" (CPTED), and other existing policing tactics would need to adapt to stay ahead of the criminals.

***Public Order***

Protesters, in illegal demonstrations, may use drones as surrogates for people by swarming the lower airspace instead of protesting on the horizontal ground. This tactic may facilitate the protesters' attempts to circumvent existing public order laws and enforcement efforts, as well as potentially disrupt legitimate drone activities (e.g. commercial) by physically occupying the lower airspace. An analogy would be how

illegal demonstrations on the ground may obstruct pedestrian and vehicular traffic along busy streets.

Drones may also be used to amplify the effects of illegal demonstrations through live-streaming, physically reach out to people at high-rise buildings, and challenge law enforcement efforts if deployed to monitor the movement of police officers. This tactic was first seen in New York in 2011 when "Occupy" protestors deployed a repurposed consumer drone to broadcast footage of protests across the globe; this effectively helped the street demonstrations to transcend geographical distances and reach out to more viewers through the online media space (Wagstaff 2011)

More profoundly, the use of drones for illegal demonstrations may be a strategic move by protestors such as anarchists to challenge the state by physically subverting its control (or perceived hegemony) of the lower airspace by taking to the air besides taking to the streets, and enhance their anti-establishment messaging by countering the public messaging by law enforcement and mainstream media. Hence, such emergent public order issues can complicate the development of policing tactics, and legislation to regulate or criminalise the use of drones (Graham 2016, pp. 23 – 25).

***Terrorism***

A terrorist drone attack on high-rise communal spaces (e.g. community gatherings at sky parks) may be used as a possible tactic to evade tight security measures (e.g. police patrols; bollards and vehicle barriers) on the horizontal ground in order to generate an alarming spectacle and panic (besides casualties) comparable to an attack (e.g. vehicle crash) on crowded streets. The September 2001 attack on the World Trade Centre in New York and the purported weaponisation of drones by terrorists may have been bellwethers of such a feared scenario (Warrick 2017). High-rise buildings, built taller and clustered closer, and incorporating facilities that draw and connect people, may present more target-rich environments to terrorists as compared to buildings that are more dispersed geographically (DHS 2011, p. 2.9).

Besides casualties, terrorists may target or sabotage high-rise facilities such as vertical farms which are crucial to sustainable growth in cities. While the possibility of terrorists (besides criminals and anti-social groups) targeting food supply as a means to harm people is not a new concern (World Health Organisation 2002), high-tech vertical farms would expand food sources beyond rural areas and into the cities, thus presenting an additional urban security concern – agro terrorism and cyberattacks - to security agencies (Khoo 2015, p. 10).

Terrorists (besides criminals) may also find it increasingly practicable to use drones instead of human agents (on the ground) for pre-attack surveillance, counter-surveillance, directing attacks, and video propaganda. The 2008 Mumbai attack, for example, demonstrated the utility of live video coverage (although unwittingly by the media) to terrorists during the course of attacks (Legal Correspondent 2012). While certain measures (e.g. geo-fencing and electronic identifier) may reduce the risk of

drone attacks by regulating the purchase and use of larger drones that can carry larger payloads, a possible gap may lie with light consumer drones which may be harder to monitor and regulate, and can perform surveillance and video streaming functions. Light drones may evade regulation as they can be acquired online and offline with ease, and can be built using parts and instructions obtained from the internet (Ohio University 2016).

Essentially, the use of drones would give terrorists and criminals a strategic edge – air capability – which was previously the preserve of the military and law enforcement (e.g. police helicopters and high-rise CCTVs). Hence, existing measures for community vigilance, and surveillance and emergency response by security agencies would need to adapt to terrorist threats against vertical communities.

***Cyberspace***

The vertical space of cities is set to grow smarter - digital and highly connected - with the proliferation of drones and smart buildings. Smart buildings (residential and commercial) - enabled by the Internet of Things (IoT/BIoT) – would see home appliances, security systems, essential services (Infocomm technology, power and water), features (lifts, lighting) and etc. connected to create a better living and working environment (Thong 2016). For example, smart building concepts have been introduced in Singapore's public housing plans (HDB, 2014).

The smart vertical space, however, may introduce additional vectors for cyberattacks that, at present, are posing a growing threat to (smart) cities. This concern stems from the increasing number of interconnected devices and systems, thus expanding the attack surface of cities to malicious acts by cybercriminals, cyber activists, and state and non-state actors (Reys 2016). Existing measures, such as indoor and perimeter CCTV cameras and physical access controls, to protect buildings and systems may not be effective against virtual intruders who can infiltrate through the vertical space where physical security and cybersecurity intertwine (Foster 2014). For example, researchers from the Ben-Gurion University of Negev, Israel, reportedly tested the use of drones to surreptitiously approach protected buildings and circumvent "air-gapping" measures that protect the computers in them in order to steal data (Dormehl 2017).

The underlying intent of cyberattacks can range from criminality to subversion given that data that permeate smart devices and systems in the vertical space would be channeled to the government's systems (Tan 2017). Indeed, the gravity of cyberattacks to nation states has driven the North Atlantic Treaty Organisation (NATO) to recognise cyberspace as the fifth domain of war (NATO 2017), in which modern cities are conceived as primary targets (Graham 2010, p. XXIV).

Given the vastness of cyberspace, cyberattacks coming through the vertical space may manifest in various forms such as:

a. Cyberattacks that use drones for "rooftop packet sniffing" – intercepting Wi-Fi/Bluetooth signals to surreptitiously monitor network traffic and steal passwords - may become more substantial as more systems and devices in buildings are connected to the city's smart infrastructure (Schureimen, West and Schurer 2016). With advances in hacking tools and drone technology, this tactic may pose a serious threat to the security and confidentiality of data (private and public) transmission from smart buildings (Bosworth, Kabay and Whyne 2009, p. 11).

b. Cyberattacks that infiltrate systems and devices in buildings can disrupt essential services such as electrical power distribution, smart lifts (vertical transportation), security CCTVs, and elderly/medical monitoring and alert systems. For example, the hacking of smart lifts may result in public fear and consequences comparable to the hacking of autonomous cars. The hacking of elderly/medical monitoring and alert system, particularly in vertical communities where there is a significant elderly population, may be comparable to ransomware attacks on hospital systems. The impact of such cyberattacks can be higher in high-rise buildings where the terrain makes emergency response more challenging, hence may necessitate the formation of municipal-level computer emergency response capabilities (Snow 2017).

c. Cyberattacks that result in "drone-jacking" (of individual commercial or transport drones) can potentially cause accidents or facilitate a crime (Aviat Drones 2017, p. 15). In addition, studies suggest that the global navigation satellite systems (GPS) can be hacked (Crampton 2016). Hence, a drone traffic management system – based on GPS - can possibly be compromised, thus resulting in economic disruptions that may be comparable to the effects from gridlocks stemming from compromised smart (road) traffic management system.

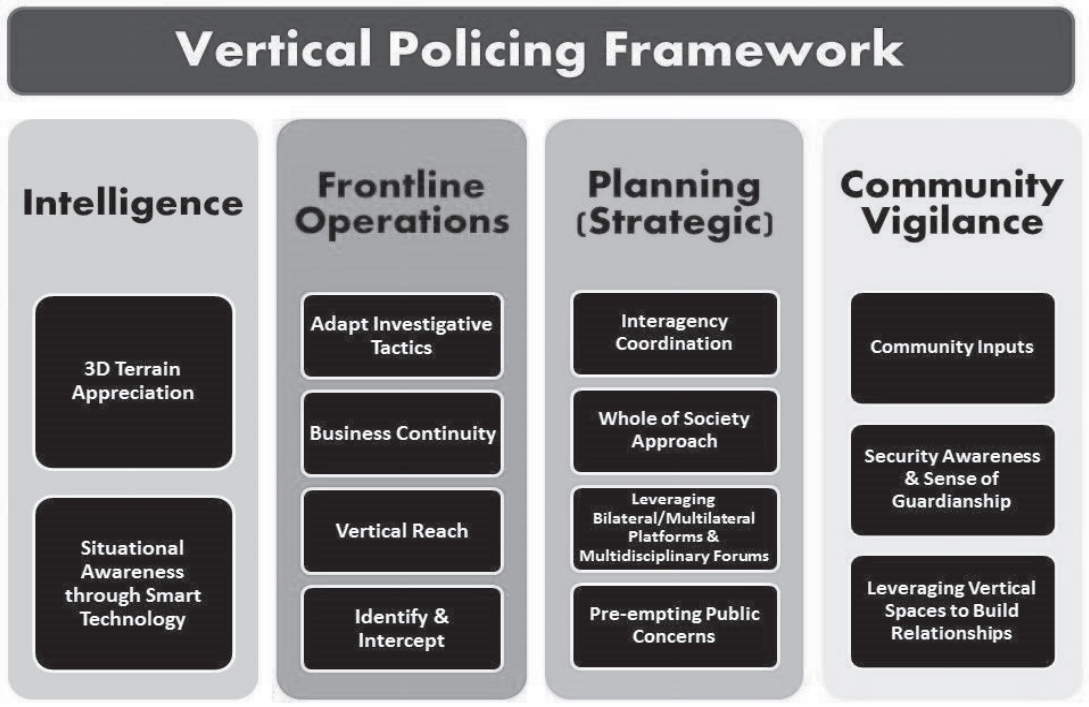
In sum, threats to the vertical space of cities would stem from adversaries (criminals, terrorists, etc.) adapting their tools and tactics in order to stay ahead of security agencies. This would involve exploiting the opportunities that come with the same features (drones and high-rise smart buildings) that enable the utilisation of the vertical space. As cities strive to protect their vertical space, they may inadvertently become more coveted as targets. A successful attack(s) would not only bring significant gains (e.g. monetary, mass casualty, reputation) for the adversaries but also leave an enduring psychological impact on the vertical communities.

## POLICY IMPLICATIONS: VERTICAL POLICING FRAMEWORK

Given the plausible security challenges in the vertical space, Singapore and other global cities would need to gird for the future by developing new policing strategies as traditional approaches for vertical patrols and neighbourhood watch may be inadequate to effectively protect the vertical space of cities. Essentially, policing strategies should be proactive in order to keep cities safe and secure even as the

spaces within growing. This would include sustaining the resilience of cities even as its demographics and socio-economic character evolve (Dodds 2017). A framework for vertical policing as shown in Figure 2 would be necessary to meet challenges from the emergent threats and may entail adapting four enduring policing strategies: intelligence, frontline operations, planning and community vigilance (Muhammad 2017a).

**Figure 2: Framework for Vertical Policing**




***Intelligence***

Intelligence-led policing has been one of the smart policing approaches adopted by cities worldwide especially since the September 2001 terrorist attack in the U.S highlighted the increasingly complex security landscape. This approach is relevant to cities both in the developed and the developing world as criminals are fast innovating by operating transnationally and exploiting new technologies (INTERPOL 2017). It leverages data for crime analysis and analytical software tools to predict criminal and anomalous activities, assesses risks and informs decision-making (Casey 2013). For example, the Los Angeles Police Department (LAPD) has the PredPol system and the Singapore Police Force (SPF) has the Computerised Criminal Intelligence System (C-CRIS) (Berg 2014; Langlois 2008, p. 151).

As the vertical space of cities expands, security agencies need to incorporate a deeper three-dimensional appreciation of the operating terrain in their crime analysis practices and analytical software tools. Threats related to crime hotspots, persons of

interest and anomalous activities including hostile drones may not be horizontally limited to the streets. Rather, these threats (including risk levels) may be shaped by the physical (e.g. building features) and socio-economic characteristics (e.g. household, commercial and organisational occupants) of the vertical space (Challinger 2008). The lower airspace where legitimate drone traffic would permeate, and (very) high-rise, mixed-use and smart buildings or infrastructure need to be constantly monitored and analysed for potential threats and vulnerabilities (Rawn 2015; Archibald et al. 2002, p. 15 – 16).

A deeper three-dimensional appreciation of the terrain may mark a paradigm shift as the vertical space would cease being perceived as crime-free and solely accessible (police helicopters, police drones, high-rise CCTVs) to security agencies for the purpose of projecting security presence and enhancing situational awareness. Security agencies need to ascertain whether any vertical space is optically or/and physically inaccessible to them, thus creating a vacuum in security (Adey 2010, p. 61). Both the vertical and horizontal spaces in cities would thus have operational relevance.

Leveraging smart technologies – police drones, high-rise CCTVs, ambient IoT sensors in buildings and etc. – which may be powered by Artificial Intelligence (AI) can enable better mobility and reach for the purposes of situational awareness and intelligence collection at the vertical space (FICCI &EY 2015, p. 17). For Singapore, there may be a need for more high-rise Police (Hawk Eye) cameras that are integrated with public housing (Smart HDB homes) and future drone traffic management system. The analysis of crime data using software tools when juxtaposed with analysis of other data from smart technologies (sensors) may help to draw useful correlations that provide actionable intelligence for security agencies (Prasad 2017).

***Frontline Operations***

Smart technologies can enhance operational capabilities – patrols and incident response, including the interception of hostile drones - for vertical policing but their efficacy is also contingent on how well policing tactics, procedures and training have been adapted to suit the vertical space. Cities which lack the capacity and resources to adopt smart technologies may leverage established mechanisms in the international law enforcement community such as INTERPOL's for support (Muhammad 2017b). The following steps for adaptation may be necessary:

a. Security agencies must ensure that their investigative tactics can keep pace with changes to criminal intent and tactics that are enabled by the disruptive technologies (e.g. "Uberisation" of drones) and features (physical and cyberspace) that may characterise the vertical space. For example, agencies can learn from contemporary challenges faced in investigating crimes that arose inadvertently from the proliferation of online social (Tinder, Grindr), ride-sharing (Uber, Grab) and space-sharing (Airbnb, Share Desk) services. This would require collaboration with stakeholders such as technology developers, building/infrastructure managers, and municipal agencies.

b. Security agencies must develop business continuity plans in the event a cyberattack(s) compromises technological tools (e.g. police drones, police CCTVs) and thus disrupt vertical policing. The plans may include leveraging (and training) community assets (e.g. neighbourhood watch members, human intelligence) as "eyes and ears on the ground" but this is predicated on cultivating good community relations and field intelligence (HUMINT).

c. Security agencies must ensure that their incident response tactics can effectively reach potential threats or situations in the vertical space. First, coordination with ground forces and community assets may be requisite given the harder-to-reach terrain. For example, Singapore has the "myResponder" mobile app which can activate volunteers in the vicinity of cardiac arrest cases while emergency responders are on the way. Second, police drones may be exempted from automated control measures for privately-owned drones such as geo-fencing and other sensors (sense-and-avoid) that help to safeguard privacy and safe distance as these may impair operational reach.

d. Security agencies must ensure that the technologies used in incident response are able to effectively establish the identity of and possibly intercept potential threats. First, police drones must be able to identify rogue/suspicious drones (e.g. via transmitted electronic identifier), similar to how intelligent street-level CCTVs are capable of automated vehicle number plate recognition (ANPR). Second, police drones may need facial/object recognition capabilities to promptly identify suspicious persons/objects detected at high-rise levels, similar to how police officers conduct checks on suspicious persons/objects at the streets. Third, police drones may require certain offensive capabilities in order to respond promptly to certain hostile incidents rather than wait for police officers to arrive.

***Planning (Strategic)***

As the lower airspace may be the bustling vertical streets of the future and thus entail the interests of multiple stakeholders, the deployment of police drones for patrols would require more strategic planning.

*Stakeholder Coordination*

First, security agencies would need to coordinate with other public agencies in order to comprehend how the lower airspace may be segmented into zones and regulated in accordance with the drone traffic management system and prevailing laws (e.g. Unmanned Aircraft (Public Safety and Security) Act), as well as the full spectrum of drone owners/users and activities. Such coordination would also help influence the development or updating of drone-related regulations and city infrastructure that can support security functions. The significance of this stems from the ever-evolving drone technology and market that would make the process of updating regulations (e.g. in relation to Singapore's Unmanned Aircraft (Public Safety

and Security) Act) and enhancing city infrastructure a constant work-in-progress (Zickuhr and Stahl 2016).

Inter-agency coordination can be part of a whole-of-society (WOS) approach to strike a balance between the diverse and possibly conflicting interests (commercial and social) of the various stakeholders; these are the drone manufacturers, civilian airspace regulator, end users (commercial, leisure/hobbyists, interest/lobby groups, public agencies), and developers and occupants/owners of private property and high-rise buildings. Social (e.g. privacy intrusion vis-à-vis freedom to use drones), technical and associated cost-sharing issues (e.g. failsafe systems, "sense and avoid" smart sensors) may converge in these interests (Mohammed et al. 2014). For example, pressures from private property owners to exclude drones from the lower airspace directly above or near their land/buildings may hinder innovations in the use of drones for commercial (and security) purposes; commercial users may politically lobby for different drone rules (Rule 2014). Safety-related rules that restrict the use of recreational drones over crowded public areas and during events may be decried by hobbyists as discriminating in favour of corporations (e.g. commercial drones by aerial photo/video service providers), and by activists as stifling public space and curtailing free speech (Kopstein 2017; Garrett and Fish 2016). For example, current regulations on the use of recreational drones in Singapore may be regarded by some hobbyists as overly restrictive (Chen 2017, p. 158)

Six specific policy issues may apply in the WOS approach to address these interests and these are: space (allotted aerial zones (horizontal and vertical) where different users can fly drones safely and minimise conflict), technology (drone features and physical infrastructure to ensure safe flight), incident management (procedures and systems to mitigate emergencies in the airspace), human factors (relevant training and licensing for different types of drone users), security controls (physical and cyber; responsibility of each stakeholder), and privacy (no-fly space and lines of property rights) (Low et al. 2014).

Given the complexity of the WOS approach, it should be undertaken by a government-led committee that is supported by working groups that look into each policy issue particularly on aspects of regulatory procedures and (technical) capacity building. These policy issues may intertwine with ongoing and upcoming smart city/nation initiatives. For example, the national ICT infrastructure that will be built over the next two decades for smart cities (and smart buildings) projects would need to incorporate a network of high-rise IoT sensors and CCTV cameras, augmented with AI and video analytics (iHLS 2017), for the purpose of supporting security functions (monitor drones and surveillance of high-rise areas/activities) on top of environmental monitoring and regulating drone traffic. An architectural website article "The Three-Dimensional City: How Drones Will Impact the Future Urban Landscape" further illustrates this point:

*"Urban three-dimensional space designed with drones in mind could address some of these obstacles by providing locations for sensors and consistent access to wireless networks for drones to maintain communications."*

*"Architects will play an important role in designing cities that appropriately respond to this unprecedented multidimensional urban space, making buildings that work to facilitate drone navigation and communication rather than inhibit it." (Rawn 2015)*

The composition of the committee and its working groups must have adequate representation from each stakeholder group to ensure that all relevant interests, including the private sector such as building developers and building owners, are fairly considered. The committee may also leverage existing bilateral and multilateral platforms (e.g. The Future of Cities and Urbanisation Agenda – World Economic Forum) and multidisciplinary forums (e.g. Future Cities Laboratory - ETH Zurich/Singapore) to engage and exchange ideas with major cities overseas that similarly anticipate vibrant vertical spaces in the long term. For example, the European Union (EU) is developing plans and standards (U-Space) – to ensure safety, privacy and security - for individuals and businesses to operate drones in the lower airspace (up to 150 metres) including in EU cities (European Commission 2016).

An exploration of the formation of this WOS approach and its key success factors, however, is beyond the scope of this paper. Nonetheless, it is important to note that certain cities, unlike city-states such as Singapore, may face more planning challenges subject to the country's structure of governance which may be multilevel and with each level having different responsibilities and considerations. For example, the U.S Federal Aviation Administration (FAA) on one hand is concerned that different state-level and local-level regulations on the use of drones could limit the efficacy of federal-level regulations to ensure the safe use of drones (FAA 2015). On the other hand, cities (i.e. local-level) may see excessive federal-level actions as stifling local economic interests and innovation (Widener 2016).

*Pre-empting Public Concerns*

Second, the deployment of police drones with offensive and AI-enabled surveillance capabilities must be calibrated as it may draw public concerns over accountability, safety, data protection and privacy (McNeal 2014). Subject to the socio-cultural context and demarcation of the lower airspace which would be determined by the drone traffic management system, certain communities may demand that security agencies secure a warrant from the court before police drones can be dispatched for surveillance and interception duties (Zaleski 2016). This legal requirement may limit the operational efficacy of police drones and delay the detection and neutralisation of threats, and may even escalate into a heated political contestation over these public concerns (Merrill and Troen 2014). Hence, security agencies require strong relationship with and support from the community – to obviate such legal requirements - for (ubiquitous) drone patrols to be effective.

*Community Vigilance*

Community vigilance would be crucial to supporting security agencies in detecting and deterring threats in the vertical space (within buildings and contiguous lower airspace). Residents and tenants in vertical communities may be aware of certain local issues that can have security implications. They can play a role in looking out for hostile drones and suspicious/unusual persons who may portend an imminent security threat to people, and smart devices and systems (ICT, essential services).

Inputs from the communities can also be instrumental in the formulation of vertical policing strategies; this would bolster the cities' resilience by facilitating the analysis of threats through information-sharing and enhancing emergency response plans (Dodds 2017). The importance of such inputs would grow with the expansion of the vertical space (e.g. mixed use buildings) at it may involve multiple stakeholders besides residents and tenants. Hence, the formulation of vertical policing strategies (e.g. emergency response and crisis communications) may be a more complicated process. For Singapore, such strategies may entail expanding the current efforts undertaken by programmes such as Neighbourhood Watch Zone (NWZ) and Citizens on Patrol (COP).

Security awareness and sense of guardianship are key elements of community vigilance (Challinger 2008, p. 3; Townsley et al. 2013, p. 16). These elements can be fostered through regular and meaningful social interactions. Ideally, the design of (very) high rise and mixed use buildings/infrastructure should translate the social interactions that occur at the horizontal space (e.g. streets and parks) into the vertical space (Hitzler 2016, p. 63).

However, challenges abound as the confluence of certain attenuating factors can potentially hamper social interactions; the following may be more significant:

a. Physical features of high-rise buildings may not facilitate social interactions among residents (and tenants) given certain constraints in building high density on limited land. Furthermore, certain physical security features in buildings may limit opportunities and space for social interactions (Townsley et al. 2013, p. 66). Nevertheless, it is increasingly crucial for urban planners and building developers to consciously plan for spaces that can facilitate social interactions given the expansion of the vertical space.

b. Socio-cultural differences in global cities that may arise due to migration from within and outside the country may hamper the cultivation of social bonds that underpin a sense of community. Such differences, if unmanaged, can result in social fragmentation that may be inimical to security. With appropriate integration strategies, such differences can be tapped as a rich diversity of cultures that may enrich social interactions (European Union 2011, p. 34).

c. Social media and digitisation of daily life, as they permeate, may reduce the need for real-life social interactions and the meaningful use of public space. While online technologies (e.g. Facebook, chat groups) can foster useful connections in the virtual space, people may spend more time in isolation (Hitzler 2016, pp. 1 - 2). Hence, online technologies can complement but cannot substitute meaningful social interactions in the physical space where communities need to exercise vigilance against real-life threats.

Given the challenges, security agencies would need to coordinate with various stakeholders in the vertical communities – such as urban planners, building developers and potential residents/tenants - from the outset. The purpose of such coordination extends beyond the inclusion of CPTED principles into the design of the vertical space, but of strategic importance, to influence the creation of spaces that can facilitate meaningful social interactions with the view of building community vigilance. The next step would be to collaborate with the relevant stakeholders in optimising the utility of the spaces (e.g. hosting community gatherings, vertical block parties) to bring people together and build up relationships (Chia 2014). This collaboration can be subsumed under the government-led WOS approach - proposed earlier in this paper - to consider the diverse interests of the various stakeholders of the vertical space.

Given that community vigilance also depends heavily on the relationship between the state and the community, such collaboration should also aim to produce programmes that promote and sustain a healthy relationship – trust and confidence - between people and security agencies. Security agencies, after all, are public institutions that perform the functions of the state. Singapore is one example of how a healthy relationship can help the people understand that community vigilance and police efforts are concomitant aspects of effective law enforcement, but other cities may face more difficult and deep-rooted relationship issues (Rosenberg, 2016). This point can also be inferred from a 2011 study commissioned by the Danish Security and Intelligence Service (PET) which noted that attitudes towards enhanced security measures are generally positive if there is a healthy level of communal trust and trust in the state (Muhammad 2017c; Nielson, Laisen and Wandorf 2016).

## CONCLUSION

The expansion of the vertical space of cities including Singapore's is a multi-dimensional matter and its security would thus require a multi-pronged approach. Homeland security agencies would need to keep abreast of and analyse the various issues and trends that may shape the plausible scenarios of vertical urbanism in order to anticipate the emergent threats (and challenges) that may permeate the vertical space. Cooperation between the security agencies of cities within countries and internationally may be instrumental to this endeavour.

Vertical policing strategies for intelligence, frontline operations, planning and community vigilance would need to adapt to meet challenges from the emergent

threats (Muhammad 2017a). Vertical policing strategies should also be proactive in order to keep cities safe and secure even as the spaces within grow.

Hence, homeland security agencies especially the Police and civil defence would need to participate in the planning and development of the vertical space of cities. This should begin with close coordination with the various stakeholders in vertical communities (public, private and residents/tenants) from the onset, given that the diverse interests of various stakeholders may result in the vertical space developing wider social, economic and political meanings with further implications on security. Such coordination can be part of a government-led whole-of-society (WOS) approach to looking into specific policy issues that address the diverse and possibly conflicting interests of the various stakeholders of the vertical space. The approach may also leverage existing bilateral and multilateral platforms and multidisciplinary forums to engage and exchange ideas with major cities overseas that similarly anticipate vibrant vertical spaces in the long term. An exploration of the formation of this WOS approach and its key success factors, however, is beyond the scope of this paper.

As the vertical space is evolving, there is also a need for further research into capacity building for the policing of the lower airspace (proliferation of drones) which would be the vertical streets of the future. Specifically, further research in terms of horizon scanning would be useful for deeper exploration into the four strategies of the vertical policing framework that was discussed earlier in this paper.

## REFERENCES

Adey, Peter, "Vertical Security In the Megacity: Legibility, Mobility And Aerial Politics." *Theory, Culture & Society* 27 (2010) 6: 51-67. http://journals.sagepub.com/doi/abs/10.1177/0263276410380943

Archibald, Rae W., Jamison J. Medby, Brian Rosen, and Jonathan Schchter, "Security And Safety In Los Angeles High-Rise Buildings After 9/11." No. RAND-DB-381-BOMA. RAND CORP SANTA MONICA CA, 2002. https://www.rand.org/content/dam/rand/pubs/documented_briefings/2005/DB381.pdf

Aviat Drones, "The Security Drones Report 2017." IFSEC Global, 2 June, 2017. https://directory.ifsecglobal.com/Drone%20Report%202017-file076075.pdf

Benites, Jason, "Policing Vertical Communities: Coming To A Suburb Near You. California Commission on Peace Officer Standards and Training, The Command College Futures Study Project." May, 2008. http://lib.post.ca.gov/lib-documents/cc/42-benites.pdf

Berg, Nate, "Predicting Crime, LAPD-Style." The Guardian, 25 June, 2014. https://www.theguardian.com/cities/2014/jun/25/predicting-crime-lapd-los-angeles-police-data-analysis-algorithm-minority-report

Browne, Ryan, "Drone Complaints Soar In The UK, Leading To Growing Annoyance And Concerns Over Snooping/" CNBC, 3 April, 2017.

http://www.cnbc.com/2017/04/03/drone-complaints-soar-in-the-uk-leading-to-growing-annoyance-and-concerns-over-snooping.html

Calder, Kent E., "Singapore: Smart City, Smart State." The Brooking Institution Press, 2017.

Carey, Bill, "Europe Advances Small Drone Regulations, 'U-Space' System, AINonline." 13 January, 2017. http://www.ainonline.com/aviation-news/business-aviation/2017-01-13/europe-advances-small-drone-regulations-u-space-system

Casey, Jessica, "Seattle's Predictive Policing Program. Data-Smart City Solutions." 11 April, 2013. http://datasmart.ash.harvard.edu/news/article/using-predictive-policing-to-reduce-crime-rate-189

Challinger, Dennis, "From the Ground Up: Security for Tall Buildings. Connecting Research In Security To Practice (CRISP)." ASIS Foundation, 2013. http://www.popcenter.org/library/crisp/security-tall-buildings.pdf

Chen, Siyuan, "The Regulatory Framework For Aerial Imaging By Recreational Users Of "Drones" In Singapore: Old And Emerging Issues And Some Possible Solutions." *Singapore Academy of Law Journal* 29 (2017) 1: 126-162.

Chia, Eliana, "Building Neighbourhood Social Resilience. City Of Vancouver, Greenest City Scholars Program." 29 August, 2014. https://sustain.ubc.ca/sites/sustain.ubc.ca/files/Sustainability%20Scholars/GCS%20reports%202014/Neighbourhood%20Social%20Resilience%20-%20Final%20GCS%20Report.pdf

Crampton, Jeremy W., "Assemblage Of The Vertical: Commercial Drones And Algorithmic Life." *Geographica Helvetica*, 71 (2016): 137-146.

North Atlantic Treaty Organisation (NATO), "Cyber Defence." NATO, 17 February, 2017. http://www.nato.int/cps/en/natohq/topics_78170.htm

DHS, "Reference Manual To Mitigate Potential Terrorist Attacks Against Buildings." Department of Homeland Security, Science and Technology Directorate, October, 2011. https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf

DHS, "DHS S&T Awards $7.8 Million For Cyber Physical System Security Research." 3 December, 2015. https://www.dhs.gov/news/2015/12/03/dhs-st-awards-78-million-cyber-physical-system-security-research

Dlodlo, Nomusa, "The Internet Of Things For The Safety And Security Of Smart Cities." May, 2016. https://www.researchgate.net/publication/303813523_THE_INTERNET_OF_THINGS_FOR_THE_SAFETY_AND_SECURITY_OF_SMART_CITIES

Dodds, Paul, "Urban Resilience: Maintaining The Flow Of Assets, Information And People In Modern Megacities." IFSEC Global, 9 May, 2017. https://www.ifsecglobal.com/urban-resilience-maintaining-flow-assets-information-people-megacities/

Dobbs, Richard, Sven Smit, Jaana Remes, James Manyika, Charles Roxburgh, Alejandra Restrepo, "Urban World: Mapping The Economic Power Of Cities. McKinsey Global Institute." March, 2011. http://www.mckinsey.com/global-themes/urbanization/urban-world-mapping-the-economic-power-of-cities

Dodge, Martin, "Vertical Urbanism And The Forgotten Plans For Heliports." Liverpool Seminar, 14 Mar, 2013.

http://personalpages.manchester.ac.uk/staff/m.dodge/forgotten-heliports-liverpool.pdf

Dormehl, Luke, "Hackers Circumvent 'Air Gap' Security With A Drone That 'Reads' The Lights On A Computer." Digital Trends, 24 February, 2017. https://www.digitaltrends.com/cool-tech/hacking-drone-led-computer/amp/

European Commission, "Drones: Commissioner Bulc Presents Plans For The Creation Of A European Drone Services Market." 23 November, 2016. https://ec.europa.eu/transport/modes/air/news/2016-11-23-drones-commissioner-bulc-presents-plans-creation-european-drone-services_en

European Union, "Cities Of Tomorrow: Challenges, Visions, Ways Forward." European Union Regional Policy, October, 2011. http://ec.europa.eu/regional_policy/en/information/publications/reports/2011/cities-of-tomorrow-challenges-visions-ways-forward

FAA, "State And Local Regulation Of Unmanned Aircraft (UAS) Fact Sheet." Federal Aviation Administration, Office of the Chief Counsel, 17 December, 2015. https://www.faa.gov/uas/resources/uas_regulations_policy/media/uas_fact_sheet_final.pdf

FICCI & EY., "SMART Policing For Smart Cities." Ernst & Young LLP, 2015. http://www.governancenow.com/files/FICCI%20Report%20-%20SMART%20Policing%20for%20Smart%20Cities.pdf

Forrest, Conner, "Global Drone Market To Hit $11.2B By 2020, Report Says." Tech Republic, 9 February, 2017. http://www.techrepublic.com/article/global-drone-market-to-hit-11-2b-by-2020-report-says/

Foster, Kevin J., "Smart Cities: Implications For Physical Security." Security Solutions Magazine, 1 May, 2014. http://www.securitysolutionsmagazine.biz/2014/05/01/smart-cities-implications-for-physical-security/

Garrett, Bradley L., and Adam Fish, "Attack On The Drones: The Creeping Privatisation Of Our Urban Airspace." The Guardian, 12 December, 2016. https://www.theguardian.com/cities/2016/dec/12/attack-drones-privatisation-urban-airspace

Graham, Stephen, "Cities Under Siege: The New Military Urbanism." Verso Books, 2010.

Graham, Stephen, and Lucy Hewitt, "Getting Off The Ground: On The Politics Of Urban Verticality." *Progress in Human Geography* 37 (2012) 1: 72-92.

Graham, Stephen, "Drone: Robot Imperium." Transnational Institute Working Papers, November, 2016. https://www.tni.org/files/publication-downloads/drones-robot-imperium-medium.pdf

Harris, Andrew, "Vertical Urbanisms: Opening Up Geographies of the Three-Dimensional City." *Progress in Human Geography* 39 (2015) 5: 601 – 620.

Housing & Development Board (HDB), "Smart HDB Homes Of The Future, Housing & Development Board, Singapore, 11 September, 2014. https://www20.hdb.gov.sg/fi10/fi10296p.nsf/PressReleases/F93B15F80588397748257D500009CE6C?OpenDocument

Hio, Lester, "NTU Researching Air Traffic Management System For Drones Including Geo-fencing." The Straits Times, 28 December, 2016.

http://www.straitstimes.com/singapore/ntu-researching-air-traffic-management-system-for-drones-including-geofencing

Hio, Lester, "Drone Deliveries To Take Off At NUS." The Straits Times, 19 April, 2017. http://www.straitstimes.com/tech/drone-deliveries-to-take-off-at-nus

Hitzler, Nina, "People Meet in Public: Social Interactions In The Vertical City." Dalhousie University, Nova Scotia, March, 2016. https://dalspace.library.dal.ca/xmlui/handle/10222/71406

iHLS, "Smart City – Convergence Of IoT And Video Analytics." Israeli Homeland Security, 17 July, 2017. http://i-hls.com/archives/77534

INTERPOL, "INTERPOL World 2017 Strengthens Resolve For International Cooperation To Address Crime." INTERPOL World, 1 August, 2017. https://www.interpol-world.com/sites/live.interpolworld2017.site.gsi.sg/files/%5BPress%20Release%5D%20INTERPOL%20World%202017%20strengthens%20resolve%20for%20international%20cooperation%20to%20address%20crime.pdf?utm_content=buffer52f0c&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer

Kabay, M.E., Seymour Bosworth, and Eric Whyne, "Computer Security Handbook. 5th Edition. John Wiley & Sons, Inc., 2009.

Khoo, Hong Meng, "Vertical Farming – An Urban Agricultural Solution." Nanyang Technopreneurship Center, 2015. http://www.ntc.ntu.edu.sg/ntcc/Documents/Full%20Version/20.%20SKY%20URBAN%20SOLUTIONS%20-%20VERTICAL%20FARMING%20-%20AN%20URBAN%20AGRICULTURE%20SOLUTION.pdf

Kopstein, Joshua, "Police Are Making It Impossible To Use Drones To Document Protests." AOL News, 28 January, 2017. https://www.aol.com/article/news/2017/01/28/police-are-making-it-impossible-to-use-drones-to-document-protes/21701948/

Langlois, Stéphane Leman, "Technocrime: Technology, Crime And Social Control." Willan Publishing, 2008.

Legal Correspondent, "Live TV Coverage Put National Security In Jeopardy, Says Bench." The Hindu, 29 August, 2012. http://www.thehindu.com/news/national/live-tv-coverage-put-national-security-in-jeopardy-says-bench/article3836676.ece

Lim, Kenneth, "A Morning with "Drones" – Report On The SMU CLE Seminar On "Using "Drones" In Singapore: An Analysis of the Unmanned Aircraft (Public Safety and Security) Act 2015". Singapore Law Blog, 28 October, 2015. http://www.singaporelawblog.sg/blog/article/143

Low, K. H., Lu Gan, and Shixin Mao, "A Preliminary Study In Managing Safe And Efficient Low-Altitude Unmanned Aircraft System Operations in a Densely Built-up Urban Environment." Air Traffic Management Research Institute, School of Mechanical and Aerospace Engineering Nanyang Technological University, 2014. http://atmri.ntu.edu.sg/Publications/Documents/Aviation_system_block/4%20A%20Preliminary%20Study%20in%20Managing%20Safe%20and%20Efficient%20Low-Altitude%20UAV%20Operations.pdf.

McNeal, Gregory, "Drone And Aerial Surveillance: Considerations For Legislatures." Brookings Institution, November, 2014.

https://www.brookings.edu/research/drones-and-aerial-surveillance-considerations-for-legislatures/

Memoori, "Smart Buildings: Cyber Security In Smart Commercial Buildings 2017 To 2021 – Market Prospects." Impacts & Opportunities, Q2, 2017. https://www.memoori.com/portfolio/cyber-security-smart-commercial-buildings-2017-2021/

Merrill, Jamie and Oliver Troen, "Drones Are Filling Britain's skies: Look Up Now To See What Is Looking Down At You." The Independent, 20 September, 2014. http://www.independent.co.uk/news/uk/home-news/drones-are-filling-the-skies-look-up-now-to-see-what-is-looking-back-down-at-you-9746459.html

Mogg, Trevor, "A UK Prison Just Switched On An Anti-Drone 'Force-Field' To Stop Illegal Flights." Digital Trends, 18 May, 2017. https://www.digitaltrends.com/cool-tech/prison-anti-drone-force-field/

Mohammed, Farhan, Ahmed Idries, Nader Mohamed, Jameela Al-Jaroodi, and Imad Jawhar, "UAVs For Smart Cities: Opportunities and Challenges." International Conference On Unmanned Aircraft Systems, IEEE, May, 2014. https://www.researchgate.net/publication/269299864_UAVs_for_smart_cities_Opportunities_and_challenges

Muhammad, Faizal, "Securing The Vertical Space Of Cities. RSIS Commentary, 22 February. 2017a. https://www.rsis.edu.sg/wpcontent/uploads/2017/02/CO17034.pdf.

Muhammad, Faizal, "Law Enforcement: Security Challenges Ahead." RSIS Commentary, 24 July, 2017b. https://www.rsis.edu.sg/wpcontent/uploads/2017/07/CO17139.pdf

Muhammad, Faizal, "Smart CCTVs For Secure Cities." RSIS Policy Report, June, 2017c.

National League of Cities, "Cities And Drones." 2016. http://uavs.insct.org/wp-content/uploads/2016/09/NLC-Drone-Report.pdf

Nielson, Anja Dalgaard., Laisen, Jesper. and Wandorf, Charlotte, "Visible Counterterrorism Measures in Urban Spaces – Fear Inducing or Not?" *Terrorism and Political Violence*, 28 (2016): 692–712.

Ohio University, "The Benefits And Challenges Of UAVs." 20 December, 2016. http://onlinemasters.ohio.edu/the-benefits-and-challenges-of-uavs/

Ong, Justin, "'Sky's The Limit' In Singapore's Bid To Become A Drone Hub." Channel News Asia, 11 November. 2016. http://www.channelnewsasia.com/news/singapore/sky-s-the-limit-in-singapore-s-bid-to-become-a-drone-hub-7714274

Prasad, Krishna, "Urban Analytics: An Artificial Intelligence (AI) Based Approach Towards Efficient City Management." LinkedIn, 26 April, 2017. https://www.linkedin.com/pulse/urban-analytics-artificial-intelligence-ai-based-approach-prasad?trk=mp-reader-card

Public Service Division, "Conversations for the Future: Singapore's Experiences with Strategic Planning (1988 – 2011)." Volume 1, 2011. http://www.csf.gov.sg/docs/default-source/default-document-library/conversations-for-the-future.pdf

Rawn, Evan, "The Three-Dimensional City: How Drones Will Impact The Future Urban Landscape." Arch Daily, 1 January, 2015.

http://www.archdaily.com/583398/the-three-dimensional-city-how-drones-will-impact-the-future-urban-landscape

Reys, Nicolas, "Smart Cities And Cyber Threats." Control Risks, 2016. https://www.controlrisks.com/~/media/Public%20Site/Files/Our%20Thinking/Urbanisation/Smart%20cities%20article.pdf

Rosenberg, Tina, "A Strategy To Build Police-Citizen Trust." The New York Times, 26 July, 2016. https://www.nytimes.com/2016/07/26/opinion/a-strategy-to-build-police-citizen-trust.html

Rule, Troy A., "Airspace In An Age Of Drones." *Boston University Law Review*, 95 (2014) 155: 155-208.

Schureimen, Sean Paul, Christian West, and Sonny Schurer, "Drones And Corporate Security: What's New In 2016?" AS Solution, 17 November, 2016. https://assolution.com/blog/drones-corporate-security-whats-new-2016/

Shaw, Ian G. R., "The Great War Of Enclosure: Securing The Skies." *Antipode,* 49 (2017) 4: 883-906.

Snow, Jackie, "Trend Micro Report Unveils Security Checklist For Smart Cities." Smart Cities Dive, 7 June, 2017. http://www.smartcitiesdive.com/news/trend-micro-report-unveils-security-checklist-for-smart-cities/444231/

Soon, Weilun, "Airbus To Run Parcel-Delivery Drone Trial, And Maybe One For Flying Taxis In S'pore." The Business Times, 24 March, 2017. http://www.businesstimes.com.sg/transport/airbus-to-run-parcel-delivery-drone-trial-and-maybe-one-for-flying-taxis-in-spore

Tan, Weizhen, "Smart Towns Need Common Standards For Data Transfer: HDB CEO." TODAY, 7 June, 2017. http://www.todayonline.com/singapore/smart-towns-need-common-standards-data-transfer-hdb-ceo

Tankard, Colin, "How Secure Is Your Building?" Smart Buildings Magazine, 22 April, 2015. http://www.smartbuildingsmagazine.com/features/how-secure-is-your-building

Teh, Cheryl, "Rooftop Farm Has Crop Of New Ideas." The Straits Times, 5 August, 2016. http://www.straitstimes.com/singapore/rooftop-farm-has-crop-of-new-ideas

Thong, Kristie, "The Rise Of Smart Buildings In Asia." Eco-Business, 1 April, 2016. http://www.eco-business.com/news/the-rise-of-smart-buildings-in-asia/

Townsley, Michael, Sacha Reid, Danielle Reynald, John Rynne and Benjamin Hutchins, "Crime In High-Rise Buildings: Planning For Vertical Community Safety." Criminology Research Advisory Council, Australia, June, 2013. http://crg.aic.gov.au/reports/1314/29-1112-FinalReport.pdf

Twelfth Parliament of Singapore, "Twelfth Parliament of Singapore, Second Session." National Archives of Singapore, 13 July, 2015. http://www.nas.gov.sg/archivesonline/data/pdfdoc/20150717002/order_paper_-_13july15.pdf

Wagstaff, Keith, "Occupy Wall Street's New Drone: 'The Occucopter'." TIME, 21 December, 2011. http://techland.time.com/2011/12/21/occupy-wall-streets-new-drone-the-occucopter/

Wall, Tyler, "Unmanning The Police Manhunt: Vertical Security As Pacification." *Socialist Studies* 9 (2013) 2: 32-56.

Warrick, Joby, "Use Of Weaponized Drones By ISIS Spurs Terrorism Fears." 21 February, 2017. https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html?utm_term=.3daff95b11f4

Wee, Lea, "Urban Farms Taking All Over Singapore." The Straits Times, 8 February, 2015. http://www.straitstimes.com/lifestyle/urban-farms-taking-off-all-over-singapore

Widener, Michael N., "Local Regulating Of Drone Activity In Lower Airspace." Chapter 19, Zoning and Planning Law Handbook, Thomson Reuters, 2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732845.

Wong, K.M. Grace, "Vertical Cities As A Solution For Land Scarcity: The Tallest Public Housing Development In Singapore." *Urban Design International* 9 (2004) 1: 17-30.

Wong, Pei Ting, "Drug Users Turning To Apps To Get Their Fix." Today Online, 7 May, 2017. http://www.todayonline.com/singapore/weekend-drug-parties-here-organised-through-dating-apps

World Health Organisation, "Terrorist Threats To Food: Guidance For Establishing And Strengthening Prevention And Response Systems." Food Safety Department, WHO, 2002. http://apps.who.int/iris/bitstream/10665/42619/1/9241545844.pdf

Zaleski, Andrew, "The Urban Drone Invasion Is Nigh." City Lab, 22 December, 2016. https://www.citylab.com/life/2016/12/the-urban-drone-invasion-is-nigh/511496/

Zickuhr, Kathryn. and Stahl, Elias, "Cities And Drones: What Cities Need to Know About Unmanned Aerial Vehicles (UAVS)." National League of Cities, Centre for City Solutions and Applied Research, 2016. http://uavs.insct.org/wp-content/uploads/2016/09/NLC-Drone-Report.pdf

RESEARCH ARTICLE

# Fintech and the Future of Finance

*James Guild* [1]

AJPA Asian Journal of Public Affairs

**Keywords**: Fintech, regulation, finance, policy, technology

**Suggested Article Citation**: Guild, James. 2017. "Fintech and the Future of Finance" *Asian Journal of Public Affairs* 10(1): p.52-65

http://dx.doi.org/10.18003/ajpa.201710

ISSN 1793-5342 (print); ISSN 2382-6134 (online),  Published by Lee Kuan Yew School of Public Policy, National University of Singapore

**ABSTRACT**

*The application of technological innovations to the finance industry (Fintech) has been attracting tens of billions of dollars in venture capital in recent years. Examples of Fintech innovations include digital cash transfer services in Kenya and India, and peer-to-peer lending platforms in China. These services, when developed in tandem with complementary government policies and regulatory frameworks, have the potential to expand financial services to hundreds of millions of people currently lacking access and to break new ground on the way finance is conducted. This is important because sustainable economic growth is strongly linked with financial inclusion. The successful adoption of Fintech to increase financial inclusion is highly dependent on competent regulatory oversight. By examining varying degrees of success in the adoption of Fintech services in Kenya, India and China this paper argues that adopting a responsive regulatory approach, rather than an overly interventionist one, is the most suitable framework for boosting financial inclusion through technological innovation.*

## INTRODUCTION

This paper will examine the impact of technological innovation on the financial sector, an industry commonly known as Fintech. The focus of the paper is on how Fintech has expanded access to finance for millions of people in developing economies, with a specific interest in the role of regulatory frameworks in facilitating that process. The paper is a qualitative analysis of three case studies that have utilised technology in the pursuit of inclusive finance: cashless payment systems in India and Kenya, and peer-to-peer lending in China.

[1] S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore. Email: jamesjor001@ntu.edu.sg.

By inductively probing the varying degrees of success across cases, the argument will be advanced that designing appropriate regulatory architecture is critical to maximizing the benefits of technological innovation. More precisely, a light regulatory touch is required in the early phases to encourage innovation and experimentation. As successful sectors and companies grow, regulators must adapt the architecture to impose stricter controls and oversight without weighing the sector down with overly burdensome compliance requirements. Excessive or poorly planned state intervention at any point in the process can be counter-productive.

The paper will begin by defining key terms, then discuss the link between inclusive finance and sustainable economic growth in developing countries. It will then highlight the potential for technological innovation to increase financial inclusion, with special attention given to the importance of regulatory architecture. After a brief discussion of methodology, the paper will move onto the case studies before concluding with a series of policy implications. Because Fintech involves the intersection of both the financial and technology sectors, how it should be regulated (as a financial instrument or a utility or something entirely different), and the appropriate design of the regulatory architecture are important puzzles for policy-makers and researchers. Those puzzles form the primary research questions this paper seeks to address, with a heavy emphasis on the public policy implications that can be drawn from the case studies.

## CONCEPTUAL FRAMEWORK

Fintech companies – defined here as companies that apply technological innovations to increase efficiency and/or expand access to the finance industry – have proliferated in recent years and are attracting increased interest from venture capitalists. In 2016, Fintech companies received $17.4 billion in global investment, 11% more than the previous year, and that number is expected to continue rising (Wintermeyer 2017). This paper will focus on Fintech innovations in two areas: cashless digital transactions and peer-to-peer lending platforms. Both areas represent examples of technology (mobile phones and the applications and software that run on them) being innovatively used by companies to satisfy previously un-met market needs. Moreover, both cashless payment systems and peer-to-peer lending platforms, when properly used, are powerful tools of inclusive finance.

This is important because there is strong evidence linking financial inclusion with sustainable economic growth. In the context of this article, financial inclusion is defined as “improving the range, quality and availability of finance services to the underserved and the financially excluded.... [This] implies that both unbanked and under-banked households and firms” receive access to banking services, like bank accounts and payment settlement mechanisms, as well as credit (Stein 2010). The literature linking inclusive financial systems with economic growth, particularly in developing countries, is substantial. Studies have consistently found a positive relationship between financial inclusion and an increase in life expectancy, literacy and per capita income (Kodan 2013; Sarma 2010). This makes intuitive sense. When

marginalised and underprivileged populations gain access to financial resources from which they were previously excluded, it creates a range of new opportunities and tends to boost income (Asongu 2016a). Policy-makers who wish to create sustainable economic growth should therefore design policies that encourage financial inclusion, and expand access to financial services as widely as possible (Nabi 2013).

One of the most effective tools for accomplishing this is through the prudent application of technology, especially the use of mobile phones to conduct banking activities (Mishra and Bisht 2013; Singh 2012; Kirui et al, 2013). While the positive effect of mobile phone penetration on expanding access to finance is well established, precisely how to design and implement effective policies has been less thoroughly investigated and is the primary subject of this paper. High quality regulatory architecture has been linked with inclusive and sustainable growth (Asongu 2016b), but there is no clear consensus on what that regulatory architecture should look like. When it comes to technology and financial inclusion, the main barriers to successful implementation are of regulatory nature, as state officials must decide whether to regulate mobile banking and peer-to-peer lending as technological or financial instruments (Klein and Mayer 2011). Furthermore, while the state can incentivise financial institutions to embrace inclusive policies (Swarmy 2010), poorly timed or conceived incentives can have a negative effect on development, as will be discussed in the cases below.

This paper seeks to inductively probe a series of cases where Fintech has been applied to increase inclusive financial development in Kenya, India and China. The goal is to specify what distinguishes an effective regulatory environment from an ineffective or potentially counter-productive one. The cases have been selected based on how effectively Fintech services were adopted in each country to create an inclusive financial environment. Kenya's M-PESA mobile banking system is possibly the most successful in the world (Buku and Meredith 2013). Similar cashless payment systems in India are popular, but not as successful and the volume of mobile banking transactions has not increased month over month as it has in Kenya, as the following case studies will show. An analysis of the regulatory architecture in each country will help explain this divergence. China's peer-to-peer lending sector has also been selected as it is a successful example of a regulatory regime adapting itself to Fintech innovations in the banking sector, specifically the way capital and credit were being allocated. An analysis of how the Chinese government adapted its regulatory architecture as the peer-to-peer lending industry grew will provide useful policy lessons for designing similarly inclusive policies, particularly with respect to how it timed the implementation of its regulations.

The case study method allows for a detail-rich, qualitative comparison (using academic analyses, contemporary media accounts and Central Bank data) of how the regulatory architecture impacted the adoption of Fintech to promote financial inclusion in each case. Explaining this variance will provide insight into what the most appropriate regulatory approach is when the goal is to broaden access to financial resources. This kind of contextual analysis is useful for explaining and understanding

the impact and adoption of Fintech in economic development (Donner and Tellez 2008). The conclusions reached in this paper will be useful for practitioners who are facing similar policy challenges, as well as researchers who can test the arguments advanced on additional cases or with quantitative models using larger sample sizes.

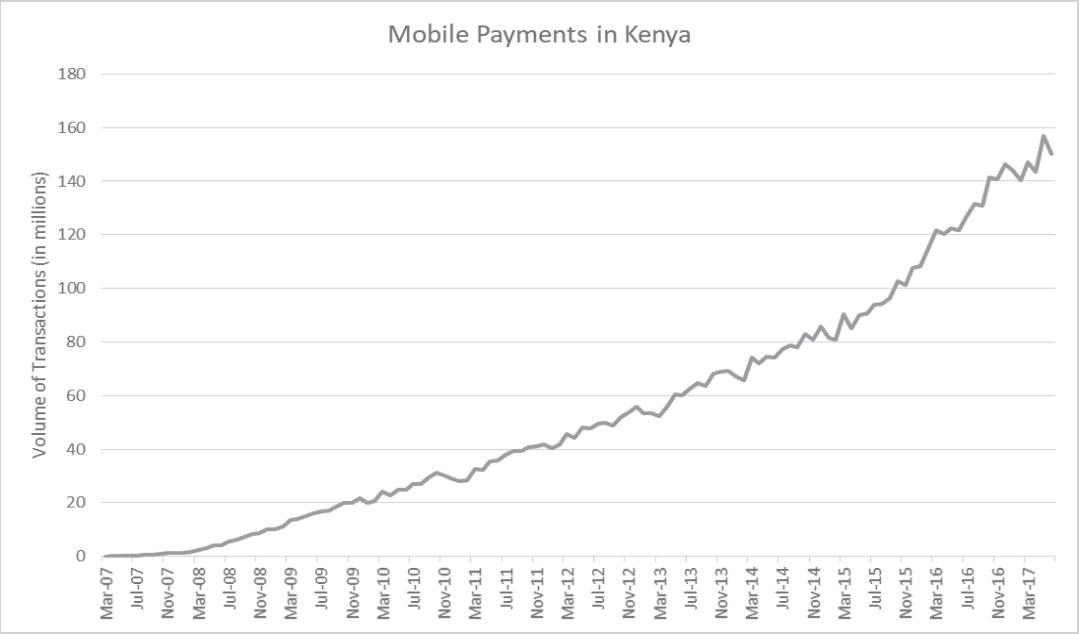
## KENYA AND THE SUCCESS OF M-PESA

In Kenya, M-PESA, a digital cash transfer service founded in 2007, is an instructive example of Fintech innovation responding to an unmet marked need. Kenyan telecom company Safaricom already had a monopoly on the telecom network in Kenya; M-PESA simply partnered with the existing network provider to add their service and by 2014 had penetrated 90% of the market. The service they offer is in high demand by consumers for its convenience and efficiency, and the infrastructure already existed to support it (Mas 2011). It simply required the right technological innovation to deliver a service that could thrive in the following conditions: many people in Kenya had cell phones but no debit cards, and poor physical infrastructure made going to the bank burdensome, particularly for rural populations. An opportunity existed for anyone who could design a technology to facilitate cash transfers using the existing telecom network and M-PESA stepped into the role. This is an example of how the Fintech industry can contribute to new frontiers in digital finance: by addressing market needs that are currently not being met through the prudent application of technology.

The advantage that these digital cash transfer services have, and the reason they can be deployed quickly and on-board millions of customers in a short period of time, is because the only real asset is the technology itself. By piggy-backing on existing infrastructure, such as Safaricom's telecom network, M-PESA could establish itself very quickly, with low start-up capital requirements and no need to invest in or build out expensive and time-consuming infrastructure (Chuen 2015). Fintech is often successfully adopted when a clever piece of technology is delivered to the existing market and fulfils an unmet need. It can gain widespread market penetration very quickly and in doing so expand financial services to millions of people.

The other important part of this story is that as M-PESA grew, the Central Bank of Kenya recognized that it needed to step in and clarify the regulatory environment. In 2009 the Bank ruled that digital payment services were not banking services, allowing for a lighter regulatory touch that helped prevent the burgeoning service from being tied down by burdensome regulations (Mwega 2014). This highlights the importance of striking the right regulatory balance at an early phase of development. Once it became clear that millions of people were using M-PESA, the Central Bank quickly decided how to regulate it, thereby eliminating confusion about the legal status of the service and under what conditions it could operate. This kind of quick and effective regulatory clarification is also present in the way Chinese regulators handled the growth of peer-to-peer lending. It is notably absent, or at least was implemented less effectively, in India with subsequently mixed results. Such regulatory clarification reduces uncertainty for investors and consumers, spells out the rules of the game and

allows technology companies to develop financially inclusive strategies with confidence. The following graph supports this interpretation.




Source: Data retrieved from the Central Bank of Kenya website, retrieved July 28, 2017,. https://www.centralbank.go.ke/national-payments-system/mobile-payments/

In 2007, the volume of mobile payment transactions in Kenya was negligible, even though a substantial market for this service existed. As M-PESA began to cater to that market, mobile transactions increased in volume. This trend accelerated after 2009 once the new regulatory architecture had been decided upon and implemented by the Central Bank. As of June 2017, there were approximately 150 million mobile transactions per month, an impressive rate of growth over ten years. This growth, and the vast expansion of access to banking services for previously un-served customers, was made possible by a Fintech company using technology to deliver a service for which there was a large demand but no means of meeting it. Furthermore, the Central Bank took prudent regulatory action at an early phase to allow M-PESA to develop and deliver this service without over-burdening it with regulatory requirements. It also quickly clarified under what conditions the service could operate. This is an instructive example of how Fintech is well-positioned to develop new modes of finance, and the important role that sound regulatory architecture plays in that process.

## INDIA AND THE CHALLENGES OF MOBILE BANKING

India is another market where a large potential for mobile banking and digital transactions exist, but is currently being under-served. As in Kenya, government officials are trying to fashion an appropriate policy framework to address this deficit, but the results have thus far been mixed.

Data from the World Bank's Financial Inclusion Data Index indicate that only 53% of adult Indians had a bank account in 2014.[2] Nearly half the adult population at that time – several hundred million people – were settling all financial transactions off the books. For a country the size of India, this represents a huge volume of economic activity that is simply never captured in official metrics like GDP or domestic consumption. It also created conditions for Fintech companies, in tandem with government policy, to on-board millions of new customers to cashless payment platforms aimed at boosting financial inclusion.

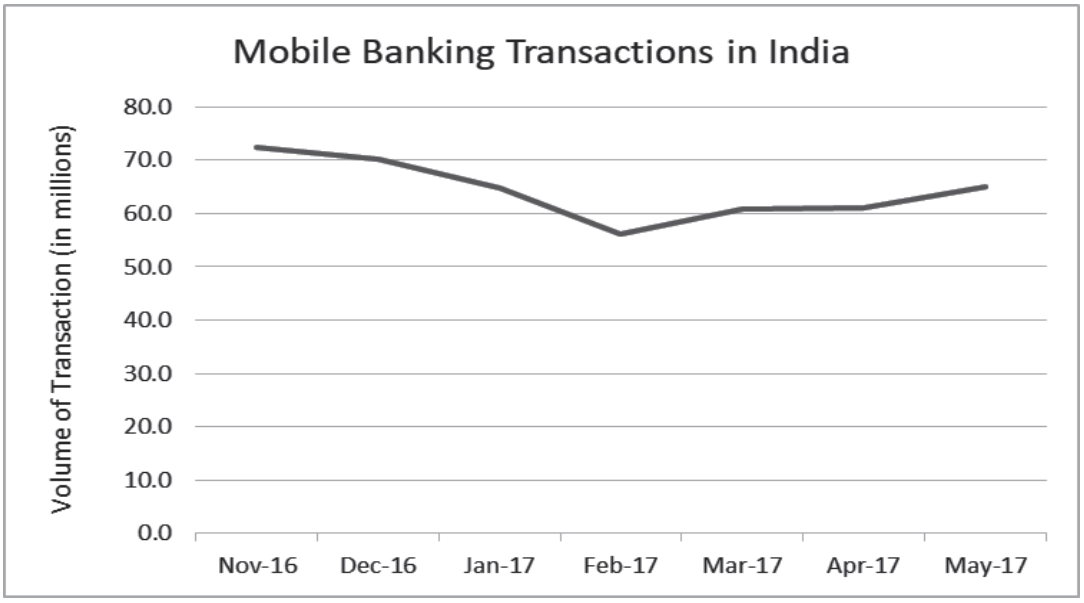
As in Kenya, Fintech companies in India are targeting this under-served demographic and offering digital financial services. The most popular is Paytm, a cashless e-wallet system that reached 200 million users in February 2017 (Variyar 2017). Part of Paytm's success can be attributed to a 2014 government programme designed to open 200 million new accounts for the unbanked poor. As the government induced more and more people to open bank accounts, the market for a digital transaction service like Paytm grew in proportion. In late 2016, demonetisation (a sweeping government program to withdraw a substantial percentage of all cash from circulation) further expanded the market for cashless transactions and Paytm received a vote of confidence in the form of a $1.4 billion investment from Softbank in May 2017 (Rai 2017). For people who may not have debit cards, but do have mobile phones, this kind of innovative technological solution embodies the potential of the Fintech industry. When it comes to meeting modern challenges of finance, leveraging technology in this way can be very effective, especially when coupled with sound public policy.

However, creating the right regulatory framework and developing appropriate policies that encourage sustainable growth without stifling innovation is a major challenge. The regulatory framework must carefully balance systemic security and economic stability with the need to allow entrepreneurial ventures room to grow and experiment. When the policies complement one another, as in the case of M-PESA and the Central Bank of Kenya, it can allow a needed service to flourish. When the government intervenes at the wrong time or with ill-considered policy or regulatory over-reach it can be, it can be counter-productive. The case of demonetisation in India at the end of 2016 is a good example of the latter.

In November 2016, Prime Minister Modi announced that all INR 500 and INR 1000[3] notes – 86% of the cash in circulation - would be withdrawn. The plan that had been in the works for several months, but was restricted to only a very small group of upper-echelon policy-makers and rolled out with little inter-agency planning or consultation (Reuters 2016). The policy was announced and implemented suddenly.

[2] Data drawn from http://datatopics.worldbank.org/financialinclusion/country/india
[3] Approximately $7.80 and $15.70 USD, respectively, as of August 1, 2017.

It was immensely disruptive and likely caused India's GDP to dip at the end of 2016 while lowered forecasts for 2017 (World Bank 2017), though growth is expected to recover. Several people may have died as an indirect result - for instance, when taxi drivers refused to take them to the hospital when they tried to pay using the now-banned notes (Banerjee 2016). For people who kept large cash reserves, particularly the rural poor and unbanked who do not keep their money in bank accounts, vast amounts of net wealth and value were wiped out. Modi stated that the goal was to target so-called black money, cash being hoarded by criminals, drug dealers and other off-book transactions, and to bring that capital into the formal economy (Kazvin 2016). And indeed, in tandem with the increasing penetration of digital finance services provided by Fintech firms, the policy has had beneficial effects. As noted earlier, the sudden withdrawal of huge amounts of cash from circulation has been a boon to digital banking and cash transfer services like Paytm. Many millions of people are now integrated into the formal economy through digital finance platforms. But the process was hugely disruptive. It wiped out much accumulated legitimate wealth, impacted millions of people's lives negatively and blunted a year of strong GDP growth. It was a policy formulated by a small group, not properly vetted and apparently did not consider the widespread disruption it would pose for the economy. This highlights why the interplay between technology innovation in finance and government policy-making is so important. In the end, demonetisation helped on-board millions of new users to digital finance platforms. But it came with real economic and human costs. Furthermore, the long-term impacts of the policy are unclear. After an initial increase in the volume of digital transactions and online banking, many consumers have seemingly returned to cash. The chart below indicates a steep drop in the volume of mobile banking transactions following demonetisation, with a gradual return to slower, more moderate growth in recent months.




Source: Data obtained from Reserve Bank of India weekly statistics, retrieved July 28, 2017, https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=39469.

This decrease in the volume of mobile banking transactions coincides with the issuance in early 2017 of new regulatory requirements for e-wallets like Payam, including stricter compliance standards, capital reserve minimums and caps on transfers to bank accounts (Moray 2017). These steps indicate that the Reserve Bank intends to regulate cashless wallet services more like a financial instrument than a strictly technological innovation. More data is needed to reach a definitive conclusion on the precise effect Indian policy-making and regulatory architecture will have on mobile banking and cashless payments in the country. But while demonetisation coincided with an initial increase in online banking, the numbers quickly dropped again while the policy itself severely disrupted the economy. This kind of inconclusive result from interventionist regulatory policies in India is not uncommon (Joseph and Varghese 2014).

## CHINA AND PEER-TO-PEER LENDING

Another area where Fintech can generate opportunities for under-served sections of the economy is through peer-to-peer lending platforms. Peer-to-peer lending platforms - mobile phone applications and software that match borrowers with lenders without a traditional intermediary, like a bank or broker - expand access to capital to millions of small business owners and consumers who historically have had to turn to usurious moneylenders, inefficient shadow banking systems or simply do without when they were unable to secure loans from traditional banks (Allen 2016). These peer-to-peer platforms are generally purveying small loans to borrowers with little collateral or no credit scores. The loans tend to be personal or for small businesses, but the amounts are so small that traditional banks have often felt it is not worth the effort to underwrite or issue them. By pooling capital from many sources, the risk of default is theoretically spread out and decentralised, rather than concentrated on a single bank's balance sheet (Lenz 2016).

The peer-to-peer lending industry has taken off in China, probably because it addressed a particularly acute structural problem in the Chinese economy: that of matching capital with borrowers. In particular, small and medium-sized enterprises have historically found it difficult to get loans from large banks which are heavily connected to or owned by the state (Wang 2004). Further, although the savings rate in China is very high, interest rates paid on bank accounts are anaemic, which drives people to seek more profitable ways to deploy their capital. Fintech innovators stepped in to match these two market participants – small business owners unable to secure loans from traditional banks, and holders of capital looking for a decent return on their savings – with one another through simple online platforms. Peer-to-peer lending platforms have rushed to capture this capital and direct it to more efficient uses, going from a single platform in 2007 to almost 2,000 today (Lin 2017)

This has had several effects. Because peer-to-peer lending is capturing so much capital, the large banks have been forced to address some of their structural inefficiencies and seek to improve the consumer experience so that they can compete with the Fintech companies (Economist 2017). It has also served an important

economic function, which is to supply capital to a wide array of economic actors who would otherwise not have access to it and improve the efficiency of allocation. This boosts consumption and small business creation, improving overall economic efficiency. It has also drawn the shadow banking system out from the shadows. China has a long history of a massive shadow banking system in which small borrowers were vulnerable to fraud and usurious interest rates. This shadow banking system has increasingly been drawn into the formal economy through peer-to-peer lending platforms (Arner 2015). This brings a largely hidden sector of the finance industry into the formal economy and subjects it to regulations and taxation, all of which is a net economic benefit.

The market for peer-to-peer lending in China has now surpassed $100 billion in value (Weinland 2017). It is no longer a small, innovative way for overlooked borrowers to get matched with the capital they need but has attracted large retail investors and reached systemic importance. The growth of the industry required a re-evaluation of the regulatory environment, and China took steps to update its policies in 2015. Like the Central Bank of Kenya, China's new regulatory approach to peer-to-peer lending is an instructive example of how sound regulatory architecture can help promote financial inclusion.

As peer-to-peer lending grew from a small section of the economy into a $100 billion industry, Chinese regulators moved quickly to clarify the industry's legal status and establish clear rules and regulations, just as the Central Bank did in Kenya with M-PESA. Many in the tech industry resisted these regulatory overtures, because the main advantage of peer-to-peer lending platforms was that they simply matched borrowers with capital, and therefore did not have to retain capital reserves of their own as the loans were not being booked on their balance sheets (Wall Street Journal 2015). This argument was valid if the industry remained small. But once Fintech firms began facilitating tens of billions of dollars in loans and courting large retail investors, it graduated to a systemically important segment of the economy. In 2015 the China Banking Regulatory Commission recognised this and imposed stricter licensing and capital requirements (Reuters 2016). Since the new regulations were imposed, the rate of growth measured in outstanding loans has slowed from 5.7 percent in July 2016 to 4 percent in March 2017, while the gross value of all loans has increased to nearly $130 billion (Lockett 2017). This indicates that the stricter regulatory requirements have not significantly impacted the growth of the peer-to-peer sector, while still ensuring a minimal standard of quality and security for the types of loans being issued.

This was accomplished through the design and implementation of prudent regulatory architecture that does not impose mandatory capital requirements or shut down non-conforming entities in an ad-hoc, abrupt or poorly considered manner, as with India's demonetisation. A tiered structure was developed that allows Fintech companies to operate in their field until they attain a certain size based on assets and volume of transactions (Arner 2015). After that, they are required to enter into a partnership with a larger, more established financial institution that is sufficiently capitalised, and submit to stricter compliance requirements.

This structure allows Fintech innovators the freedom to experiment when they have limited assets, and limited potential to create systemic risks. If their business model is successful, that success will beget additional regulatory scrutiny, which is sensible in the finance industry when billions of dollars are at stake. Tougher licensing requirements and oversight is also intended to discourage fraud, which has become an increasingly acute problem as the industry grows (Weinland 2017). While tighter regulatory scrutiny may hamper the freewheeling, style favoured by Fintech companies, when it comes to finance innovation should not be left unchecked indefinitely. The Chinese authorities created a more stable regulatory environment for the peer-to-peer sector, and it does not appear to have had a disruptive effect on the economy or dramatically slowed the rate of growth in the industry. This appears to be another example of striking the appropriate regulatory balance by responding to changing circumstances as they develop, rather than forcefully intervening through policy.

## CONCLUSION AND POLICY IMPLICATIONS

Technological innovation has the potential to revolutionise global finance by making it more inclusive, decentralised and egalitarian. A report by McKinsey estimates that advances in Fintech can potentially expand digital banking to 1.6 billion people in emerging economies and increase the volume of loans extended to individuals and businesses by $2.1 trillion by 2025 (Manyika et al. 2016). Fintech's greatest asset is that it is nimble and can deployed to leverage existing infrastructure and government policies to make finance more inclusive. This is important for the future of finance, as inclusive finance is strongly linked with sustainable economic growth.

But successful adoption of financially inclusive policies also requires striking an appropriate regulatory balance: one that encourages innovation and growth in new industries and technologies, while also clarifying regulatory requirements and developing policies that ensure stability and a minimal standard of systemic security as those sectors grow. In Kenya, M-PESA did this by capitalising on existing mobile phone penetration in the country. As the service rapidly grew, the Central Bank of Kenya made a timely decision to regulate it primarily as a telecom, excusing it from burdensome capital and compliance requirements. This clarified regulatory confusion and allowed the service to confidently pursue an expansion strategy. It now has reached approximately 90% of the population, spearheading a massive expansion of access to financial resources and banking services.

A similar sequence of events occurred in China, with regard to the peer-to-peer lending industry. In its initial phase, peer-to-peer mobile applications used technology to match relatively small-scale borrowers with lenders, thereby servicing portions of the population that had been neglected by traditional financial intermediaries, like commercial banks. In this early phase of development, Chinese regulators took a relatively hands-off approach, establishing guidelines that only imposed strict regulatory requirements once outstanding loans reached a certain threshold and

posed a systemic vulnerability. In 2015, as the sector reached $100 billion in assets, regulators imposed stricter rules, but did so in a measured way that phased in compliance standards and capital requirements over time. This forced the sector to become more structured and less vulnerable to fraud and instability without significantly reducing growth, although additional data collected over time will be needed to reach a definitive conclusion.

These two cases are usefully compared with the policy approach in India. Like Kenya, India also has a large rural population lacking access to basic banking and financial services. Also like Kenya, Fintech companies have developed innovative ways to expand banking services to those populations through mobile phones and mobile applications. To incentivise the adoption of these Fintech services, Indian policy-makers implemented many initiatives designed to encourage people to stop using cash and switch to online banking and digital payment services. The results have been mixed. Cashless transactions have increased in net terms. But in the case of demonetisation, the policy incurred substantial economic disruption and it is unclear how much it contributed to increasing online banking and cashless transactions as the volume of online banking transactions quickly subsided within a few months of demonetisation, for instance).

Although more data will help establish these findings more thoroughly and elaborate on them, the analysis of these cases suggests that attempts to force the issue by driving people toward Fintech services with blunt policy tools can be counter-productive. In Kenya and China, Fintech industries were allowed to develop at their own pace and once they posed a systemic risk or required regulatory clarification, the relevant authorities did so in response to the natural trajectory of each sector. In India, the government took a more pro-active and interventionist approach that caused significant economic disruption without yielding any clearly positive result. From a public policy perspective, this indicates that designing effective regulatory architecture for inclusive finance is best conceived of as a responsive action. That is to say, governments should allow Fintech companies to pioneer new services and technologies to meet un-met market needs, employing a relatively light regulatory touch in the early phase. As new services prove their utility and grow, regulators should respond to the specific demands of these new markets as they emerge (by providing regulatory clarity and establishing minimum standards of stability and security tailored for that market, for instance). The analysis conducted here suggests that intervening too forcefully to shape the market through policy-making and regulatory intervention can produce unwanted effects, with no guarantee that the policy goal of expanded access to finance will be achieved.

## REFERENCES


Allen, Franklin, Asli Demirguc-Kunt, Leora Klapper and Maria Soledad Martinez Peria, "The Foundations of Financial Inclusion: Understanding Ownership and Use of Formal Accounts." *World Bank Policy Research Working Paper No. 6290*, 2016. https://ssrn.com/abstract=2188803 (Accessed July 28 2017)

Arner, W. Goudlas and Janos Barberis, "FinTech in China: From the Shadows*?" Journal of Financial Perspectives* 3 (2015): 78-91.

Asongu, Simplice A., and Jacinta C. Nwachukwu, "Recent Finance Advances in Information Technology for Inclusive Development: A Survey." *African Governance and Development Institute*, 2017.

Asongu, Simplice A., and Jacinta C. Nwachukwu, "Mobile Phone Penetration, Mobile Banking and Inclusive Development in Africa." *The African Finance Journal* 18 (2016a) 1: 34-52.

Asongu, Simplice A. and Jacinta C. Nwachukw, "The Role of Governance in Mobile Phones for Inclusive Human Development in Sub-Saharan Africa." *Technovation* 55 (2016b) 56: 1-13.

Banerjee, Kritika, "25 Deaths in a Week: PM Modi's Demonetisation Drive Takes a Toll on Aam Aadmi." *India Tod*ay, November 15, 2016. (Accessed July 28 2017)

Buku, Mercy W. and Michael W. Meredith, "Safaricom and M-PESA in Kenya: Financial Inclusion and Financial Integrity." Washington Journal of Law, Technology and Arts 8 (2013) 3.

Central Bank of Kenya. Mobile Payment Database. 2017. https://www.centralbank.go.ke/national-payments-system/mobile-payments. (Accessed July 28 2017)

Chuen, David Lee Kuo and Ernie G.S. Teo, "Emergence of FinTech and the LASIC Principles." *Journal of Financial Perspectives* 3 (2015): 24-36.

Donner, Jonathan and Camilo Andres Tellez, "New Perspective on Development Communication – Emerging Technologies, Shifting Paradigms: Linking Adoption, Impact and Use." *Asian Journal of Communication* 18 (2008) 4: 318-332.

Jack, Billy, "M-Pesa Extends Its Reach." April 5, 2012. GSMA blog post. https://www.gsma.com/mobilefordevelopment/programme/mobile-money/m-pesa-extends-its-reach (Accessed July 28 2017)

Joseph, Jisha and Titto Varghese, "Role of Financial Inclusion in the Development of Indian Economy." Journal of Economics and Sustainable Development 5 (2014) 11.

Kazmin, Amy, "Modi to Crank Up Campaign Against India's Black Money." *The Financial Times,* December 26, 2016. (Accessed July 28 2017)

Kirui, Oliver K., Julius J. Okello and Rose A. Nyikal, "Impact of Mobile Phone-Based Money Transfer Services in Agriculture: Evidence from Kenya." *Quarterly Journal of International Agriculture* 52 (2013) 2: 141-162

Klein, Michael and Colin Mayer, "Mobile Banking and Financial Inclusion: The Regulatory Lessons." *World Bank. Policy Working Research Papers*, 2011. https://elibrary.worldbank.org/doi/abs/10.1596/1813-9450-5664 (Accessed July 22 2017)

Kodan, S. Anand and Kuldip S. Chhikara, "A Theoretical and Quantitative Analysis of Financial Inclusion and Economic Growth." *Management and Labour Studies* 38 (2013) 12: 103-133.

Lenz, Rainer, "Peer-to-Peer Lending: Opportunities and Risks." *European Journal of Risk Regulation* 7 (2016) 4:688-700.

Lin, Xuchen, Xialong Li and Zhong Zheng, "Evaluating Borrower's Default Risk in Peer-to-Peer Lending: Evidence From a Lending Platform in China." *Applied Economics* 49 (2017) 35: 3538-3545.

Lockett, Hudson, "China P2P industry lending nears Rmb 1tn despite crackdown, new regulations." *Financial Times,* April 4, 2017. (Accessed July 28 2017)

Manyika, James, Susan Lund, Marc Singer, Olivia White and Chris Berry, "Digital Finance For All: Powering Inclusive Growth in Emerging Economies." *McKinsey Global Institute*, 2016.

Mas, Ignacio, and Dan Radcliffe, "Mobile Payments Go Viral: M-Pesa in Kenya." *Journal of Financial Transformation* 32 (2011): 169-182.

Mishra, V., and S. S. Bisht, "Mobile banking in a developing economy: A Customer-centric model for policy formulation." *Telecommunications Policy* 37 (2013) 67: 503-514.

Moray, Deepali, "RBI's new guidelines for wallet services: strict regulations, customer security, access to interoperability, and more." *BGR,* March 24, 2017. http://www.bgr.in/news/rbis-new-guidelines-for-wallet-services-strict-regulations-customer-security-access-to-interoperability-and-more/ (Accessed July 22 2017)

Mukherjee, Andy, "Fintech's Coming to Trounce India's Banks." *Bloomberg*, May 21, 2017. (Accessed July 28 2017)

Mwega, Francis M., "Financial Regulation in Kenya: Balancing Inclusive Growth with Financial Stability." *Overseas Development Institute Working Paper 407,* 2014.

Nabi, M. S., "Role of Islamic Finance in Promoting Inclusive Economic Development." *Global Sustainable Finance Conference 2013*, Germany (4th to 5th July 2013), http://www.wfdfi.net/wp-content/uploads/2013/09/6- Mahmud_Nabi.pdf (Accessed July 22 2017).

Rai, Saritha, "Paytm Raises $1.4 billion from SoftBank to Expand User Base." *Bloomberg*, May 18, 2017. (Accessed July 28 2017)

Reserve Bank of India. "Weekly Bulletin." *2017.* https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=39469 (Accessed July 28 2017)

*Reuters*, "Here are Some of China's New Rules on P2P Lending." August 24, 2016. (Accessed July 28 2017)

*Reuters*, "Who Knew? Modi's Black Money Move Kept a Closely Guarded Secret." December 8, 2016. (Accessed July 28 2017)

Singh, A. B., "Mobile banking based money order for India Post: Feasible model and assessing demand potential." *Procedia - Social and Behavioral Sciences* 37 (2012): 466-481.

Stein, Peer, "Towards Universal Access: Addressing the Global Challenge of Financial Inclusion." The *World Bank Group*, May 21, 2010. http://siteresources.worldbank.org/DEC/Resources/84797-1275071905763/Inclusive_Finance-Stein.pdf Accessed June 15 2017.

Swamy, Vighneswara, "Financial Development and Inclusive Growth: Impact of Government Intervention in Prioritised Credit." *Zagreb International Review of Economics and Business* 13 (2010) 2: 55-72.

*The Economist*, "In Fintech, China Shows The Way." February 25, 2017. (Accessed July 28 2017)

Variyar, Mugdha, "Paytm Wallet Reaches 200 Million Users." *The Economic Times*, February 28, 2017. (Accessed July 28 2017)

*Wall Street Journal*, "China Lays Out Rules for Peer-to-Peer Lending Platforms." December 28, 2015. (Accessed July 28 2017)

Wang, Yanzhong, "Financing Difficulties and Structural Characteristics of SMEs in China." *China and World Economy* 12 (2004) 2.

Weinland, Don, "China P2P Lenders Braced for Regulatory crackdown." *Financial Times,* January 9, 2017. (Accessed July 28 2017)

Wintermeyer, Laurence, "Global FinTech VC Investment Soars in 2016." *Forbes*, February 17, 2017. (Accessed July 28 2017)

World Bank Working Paper, "India's Economic Fundamentals Remain Strong; Investment Pick-up Needed for Sustained Growth." May 29, 2017. http://www.worldbank.org/en/news/press-release/2017/05/29/india-economic-fundamentals-remain-strong-investment-pick-up-needed-sustained-growth-says-new-world-bank-report (Accessed July 28 2017)

RESEARCH ARTICLE

# The Era of Ubiquitous Listening: Living in a World of Speech-Activated Devices

***Jennifer Yang Hui and Dymples Leong***[1]

**Keywords**: speech-activated technology, privacy, human-computer interaction, behaviour norms, security

**Suggested Article Citation**: Hui, Jennifer Yang, and Dymples Leong. 2017. "The Era of Ubiquitous Listening: Living in a World of Speech-Activated Devices." *Asian Journal of Public Affairs* 10(1): p.66-84

http://dx.doi.org/10.18003/ajpa.201711

ISSN 1793-5342 (print); ISSN 2382-6134 (online), © The Author 2017. Published by Lee Kuan Yew School of Public Policy, National University of Singapore

**ABSTRACT**

*Amazon's home assistant, Echo, became a key piece of evidence in a 2015 murder case as the device was believed to be recording crucial conversation on the night of the victim's death. In the 'era of ubiquitous listening', where devices constantly scan for user voice command to perform tasks, violation to privacy results from user's response to smart technology. This exploratory paper examines behavioural vulnerabilities that are prone to exploitation in the adoption of speech-activated home assistants and considers the implications in terms of privacy challenges arising from mass adoption of the technology. Anthropomorphism is a behavioural trait that leads to the likelihood of speech-activated devices being exploited. It encompasses factors such as intonation cues, visual cues, convenience, and sociability. Habituation to the presence of speech-activated home assistants gives rise to challenges to user privacy and security. For practitioners, legal provision must be made to accommodate potentially ubiquitous speech-activated technology.*

## INTRODUCTION

Amazon's home assistant, Echo, became the unwitting star of a 2015 murder case as the device was believed to be recording key conversation on the night of the victim's death (Buhr 2016). Initially designed to improve the quality of lives of the

[1] *Jennifer Yang Hui is an Associate Research Fellow (Email: isjennifer@ntu.edu.sg) and Dymples Leong is a Senior Analyst (Email: isdsyleong@ntu.edu.sg) at the Centre of Excellence for National Security (CENS) of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University.*

general public, the unforeseen consequences of intelligent technology are becoming obvious over time. In what the MIT Technology Review called the 'era of ubiquitous listening' (Talbot 2013), devices constantly scan for user voice command to perform tasks instead of requiring manual forms of control such as hardware button. Voice recognition technology is key to this development. The ability of machine to 'listen' is a step towards making human-machine interface seamless. Voice as interface is seen as more intuitive for humans compared to the current keyboard-mouse combo input interface (Canny 2016). Voice recognition capability of devices has advanced. Google Home, for instance, is now able to recognise and support up to six different user voices (Townsend 2017). Although imperfect - voice recognition accuracy is affected by background noise as well as recording quality and may not be able to comprehend certain accents (Calore 2017; Bhagat 2016), consumers have been able to interact via speech with a range of devices for a number of years. Apple's Siri, which was launched in October 2011, was the first widely used speech recognition for smartphones. At the time of writing, Siri has been incorporated into Apple's first ever home assistant, HomePod (Pardes 2017). In November 2014, Echo was introduced to the American public. In 2016, Google launched several apps that incorporate audio interactive technology: (a) Assistant (a voice-enabled virtual assistant); (b) Home (a device that allow home owners to chat with Google search assistant and other home devices using voice commands); (c) Pixel (its first ever smartphone); and (d) Allo, a messaging app that incorporates Assistant as well as uses smart photo recognition technology and non-text based communication (emojis) (Fitzsimmons 2016).

With advancements in artificial intelligence (AI), voice recognition capability is projected to improve in future. In a lecture, machine learning expert Andrew Ng noted that speech recognition capability has progressed – though incremental (4%), this has the potential to change the way users interact with technology (Singularity Lectures 2016). Microsoft, for example, had developed a new speech recognition technology that can transcribe conversation speech as well as professional human transcriptionist, with a word error rate of 5.9% (Galeon 2016). IBM's Watson AI computer is now better able to recognise conversational speech, with the word error rate down to 6.9% from its previous record of 8% (Takahashi 2016; Saon 2016).

'Conversations' between humans, as well as between humans and devices/machines, will be transformed by AI. By 2018, technology research company Gartner predicted that 30% of interactions will be conducted through "conversations" with smart machines (Gartner 2015). Ng, for example, believed that advancement in voice recognition will alter the way users relate to technology the same way that Apple revolutionized how users interact with devices through its introduction of touch screen (Singularity Lectures 2016).

The market for speech-activated smart technology is currently niche, but poised for growth. Speech-activated devices are set to become an integral part of consumers' lives by becoming the technology underpinning smart home systems in the near future. Industry projections shows that demand for speech-activated technologies will rise steadily over the next few years, as the market for global speech-

activated devices is expected to be worth US$7.9 billion by 2024 (Transparency Market Research 2016).

A U.S. study found that millennials (up to 43% in 2016) were more likely to engage in interactions with various forms of voice and speech technologies devices on a daily basis (Hamilton 2016). Furthermore, voice-controlled smart home devices will account for nearly 30% of Americans' smart home spending by 2021. While the U.S. and Europe form the dominant market for speech-activated technology, its adoption is set to rise in the Asia-Pacific region. The adoption rate for speech-activated devices will be significantly accelerated by advancements in speech-activated technologies (Gartner 2016) and the devices' ability to provide a host of complex user interactions (e.g. integration with businesses, language and other skills). The growth of speech-activated devices raises important questions regarding behavioural norms which extend to privacy and other issues for the future. Implications of such close, personalised interaction with users are manifold.

This paper explores behavioural vulnerabilities that are prone to exploitation in the adoption of speech-activated personal assistants and considers the implications in terms of privacy challenges arising from mass adoption of the technology in future. As an exploratory piece, it considers future possibilities of an emerging form of technology in terms of scenarios. The first part of the paper will outline what 'smart' technology entails and how speech-activated personal assistants fit into the scheme of intelligent technology. The paper will then examine the impact of speech-activated home assistants on human emotions. Users relate to voice technology as they would in any human-to-human social situation, placing trust in the devices. It argues that anthropomorphism of speech-activated home assistants encompasses factors such as intonation cues, visual cues, convenience, and sociability. It will follow up by exploring potential challenges of living among speech-activated technology. Unintentional as well as deliberate exploitation of behavioural vulnerabilities resulting from user habituation to speech-activated technology will impact the society on a wider scale. The paper then concludes by pondering over how both public and private sectors should respond to a future where intelligent speech-activated home assistant is widely embedded in the society.

## METHODS

This exploratory paper seeks to find out the privacy implications of mass adoption of speech-activated personal assistants. Being a largely U.S.-based phenomenon, the devices are rarely found outside the American and European continents (Nelson 2017). Furthermore, given the fact that speech-activated technology is an emerging field, its full implications in terms of privacy and security are currently unclear. Therefore, the scenarios outlined in this paper are exploratory in nature and seek to describe future possibilities.

This study employs qualitative research methodology. Data related to speech-activated technology was collected from news articles and video-based speeches.

Official company websites and press releases are the primary means by which technology companies notify the public about their newest products. The views of top-tier technology experts can also be widely found in news reporting as well as public lectures broadcasted via online video-streaming websites. Given the nascent nature of the topic, news briefs, video broadcasts and online reporting on speech-activated technology are therefore seen as the most appropriate medium for up-to-date information on the rapidly changing area of innovation. The analysis of this research is supplemented by secondary sources such as academic literature, technological reports, and grey literature.

There is a caveat to this approach. The extrapolation of present developments to the future will likely prove to be mistaken (Gray and Hovav 2011). Given that consumer behaviour, organisational practices and policies as well as the technology itself will alter how people use technology, future directions tend to be difficult to discover in advance (Gray and Hovav 2011). For instance, the usage of speech-activated devices may not be widely adopted by individuals who hold deep-seated resistance towards new or emerging technologies. Technological Luddites (those who oppose the arrival of new and disruptive technology) and late adopters may have reservations in utilising emerging technologies. Some individuals might not consider incorporating such devices into their lives at all. Efforts to encourage or facilitate the adoption of these devices would serve to further reinforce or even intensify resistance to speech-activated technologies. Thus, news reports and even expert analysis of presently emerging technology may prove inaccurate in assessment of future trends.

## LITERATURE REVIEW

Speech-activated home assistant is a form of smart technology. Smart technology refers to technology that employs intelligent sensors to infer the state of its surroundings and is capable of modifying its behaviour to provide for the needs of their users (Elwood 2008; Zoughbi and Al-Nasrawi 2015). It learns from its experience to improve subsequent performance and interaction with users (Zoughbi and Al-Nasrawi 2015). Being 'smart' is not only a matter of ability to anticipate user needs, but also about design, which must fit seamlessly into the lives of users. A smart home, for example, has the ability to sense the needs of its occupants through inconspicuous and unobtrusive technological design that is well-integrated within the home design (Soro et al. 2016). Furthermore, smart technology engenders emotional attachment from its users: '…intelligence is not merely a matter of practicality; it is also a matter of affection (Taylor et al. 2007).'

## ANTHROPOMORPHISM OF SPEECH-ACTIVATED DEVICES: A VULNERABILITY

As speech-activated devices such as Amazon's Echo and Google Home become ubiquitous, viewing them as an addition or a member to the family will become an accepted societal norm. For instance, children may increasingly turn to Echo for assistance or companionship as they would with a human, thereby engendering a certain kind of affection for it (Mims 2016). Anthropomorphism humanises these

devices by attributing human characteristics or behaviour to them. Prolonged interactions allow for more relaxed and natural conversations as humans become comfortable with voice assistants that embody humanistic traits (Li and Lai 2001). User reviews have testified to the benefits of having Echo as a companion for individuals, especially for individuals experiencing issues in their personal relationships such as the death of a close friend (Amazon 2017a; Duran 2016).

Anthropomorphism is a behavioural trait that leads to the likelihood of speech-activated devices being exploited. It encompasses factors such as (1) Intonation Cues; (2) Visual Cues; (3) Convenience; and (4) Sociability.

***Intonation Cues***

Intonation cues increase anthropomorphism of speech-activated devices. Imbuing voice assistants with the ability to intonate clearly will enable nuanced expressions that increase trust between a user and the device. Individuals are deeply affected by the words and the tonality of a speaker. Voice pitch has considerable influence in human-computer interaction. For example, it has been noted that both males and females with lower-pitched voices project a more commanding presence and therefore engender respect (Kloftstad et al. 2016). Voice pitch influences individuals consciously and subconsciously in everyday decision making, even impacting political choice – research has found that electoral candidates with lower voices stood a higher probability in winning elections (Kloftstad et al. 2016). Therefore, imbuing speech-activated products with intonation cues will increase user affection towards the devices.

One way in which companies such as Amazon and Microsoft appeal to users' emotions is through the usage of female voices with moderately low inflections in their products. A 2011 research showed that feminine voices sound warmer and welcoming towards both male and female respondents (Mitchell et al. 2011). Amazon Echo's voice service, Alexa, was selected after tests that compared several voices with customers and focus groups (Stern 2017). The companies' approach appear to work, as many Amazon Echo and Dot users have begun to refer to Alexa in female terms, calling it a 'she'.

Providing appropriate name for speech-activated devices also increases trust and enjoyment in using the devices. For example, the spoken keywords to activate the devices make a difference to users' emotions (Ramakrishnan and EI Emary 2012). Calling the machine 'Alexa', for example, elicits more intimate reaction as compared to saying 'Okay, Google'. The latter lacks a personal name and is therefore perceived as detached (Milanesi 2017). Thus providing appropriate terms of reference to the speech-activated devices makes a difference in users' perceptions that influence interaction and ultimately, trust.

Anthropomorphism is also increased as speech-activated devices learn to speak in a more natural, human-like manner. Developers can now code more natural verbal

patterns into speech-activated devices. For instance, Amazon upgraded Alexa's verbal ability in May 2017, designing it to speak in a natural, human-like manner that sounds less robotic (Stinson 2017). Alexa is able to pepper her conversations with quirks (also known as 'speech-cons') when speaking (Stinson 2017). Coders are also developing humorous responses towards common questions in attempts to further ingratiate these assistants in users' lives. The ability to harvest data on user sentiment from voices also improves the performance of speech-activated devices. By evaluating users' speech patterns, vocabularies and preferences, Alexa, for example, is able to become increasingly attuned towards the emotional undertones in various user requests (Stinson 2017). In time, these devices could detect, infer and react appropriately to a range of emotions such as annoyance or hesitation from users (WIRED Staff 2017). Furthermore, speech-activated devices are now able to learn from previous user interaction. With these developments, speech-activated technology is increasingly viewed as natural extensions of individuals, thereby increasing anthropomorphism.

***Visual Cues***

The design and appearance of speech-activated devices make a difference to users' perceptions and are therefore crucial factors that will lead to adoption of these devices. Research has shown that aesthetics is an aspect that influences human-computer interaction. A higher rating for the aesthetics of computer device is shown to lead to an increase in general users' satisfactions and perceived usability of the device (Payne et al. 2011). This finding echoes the observation that human beings generally perceive attractive individuals to be more competent than less attractive peers and tend to assign positive attributes to them (Guye-Vuillème et al. 1999). Consequently, the sleek and stylish appearances of devices such as Amazon Echo and Google Home likely result in perceived high competency and other positive traits that will result in their adoptions by the users.

Visual cues also result in ease of usage of speech-activated devices. For example, Amazon Echo's LED light turns blue when 'woken up' by user' spoken command, providing visual indication that makes the reactions of speech-activated devices visible and easily understood by users. Soon, Echo will become visual-based as well as auditory. Amazon has unveiled plans for a touch-screen Echo device known as Echo Show, which will display users' to-do list on a screen (Amazon 2017b; Amazon 2017c). Visual cues therefore increase the mode by which users can interact with speech-activated devices that will lead to their adoptions.

***Convenience***

The convenience that speech-activated home assistants provide also engenders trust in human users, increasing anthropomorphism. The ability to connect to third-party applications optimises usability and convenience for users. This gives users more time on hand and frees up cognitive bandwidth to attend to other priorities in life. It

also reduces the obstacles (or so-called 'friction costs') for the adoption of pro-social decisions (Kahneman 2011; Service 2014; Levithin 2014).

The reduction of 'cognitive taxation' in users' daily tasks meant that speech-activated home assistants become an integral part of their lives (Sullivan 2016). For instance, the incorporation of Alexa in Ford cars allows drivers to simultaneously obtain geographical directions and compile grocery shopping lists whilst driving (Waters 2017). Children are also able to ask these devices a wide variety of information, making them useful for educational purposes (Rosenwald 2017). Meanwhile the elderly can receive timely audio reminders for their daily medicine intake by saying simple phrases such as: 'Alexa, medicine' to an Echo device (Perez 2017). These can greatly relieve the cognitive load required on parents and caregivers when caring for the children and/or the elderly, leading to reliance and trust in the technology (Busatlic et al. 2017).

***Sociability***

Speech-activated technologies can empower individuals in various pro-social initiatives. For example, speech-activated home assistants can be used as digital counsellors in place of human listening ear. Users have found that such devices become close confidantes when they feel lonely or sad. For example, a recent widower found solace in Alexa as it was able to alleviate his loneliness (Paul 2017). Such usage intensifies emotional affection towards speech-activated devices. An Echo reviewer explains that Alexa is 'patient, present, [and] listening', alleviating the loneliness and negativity that the reviewer was facing (Amazon 2017a). Another customer review on Amazon stated that Alexa helped him overcome his sadness by responding to him when he broke up with his ex-girlfriend (Bowles 2016). The ability of speech-activated home assistants to assist users in pro-social initiatives will thus contribute towards trust in the devices.

## POTENTIAL CHALLENGES IN THE ERA OF UBIQUITOUS LISTENING

While speech-activated technology enhances quality of life, concerns persist. As behaviour norms change, there will be consequences, both intended and unintended. Ramifications result from user habituation to speech-activated technology. Users of speech-activated home assistants become increasingly comfortable with them, gradually no longer noticing their presence. A term borrowed from the fields of psychology and biology, habituation refers to the process whereby an organism's body and behaviour stop responding to stimulus in a process of adaption to its environment (Hagsall 2015; Qiu and Benbasat 2009). The seamless assimilation of home assistant to the lives of its owner is an aspect that is also actively encouraged by the technology companies themselves, who advertise the devices as being a 'natural' part of the family. For example, the advertisement for Amazon U.K. showed the device reading bedtime story to the child in the family, suggesting ingredients for cooking and setting the alarm clock, essentially performing tasks that make them an integral part of the household.

The placement of voice-interactive devices in the privacy of a home entails implicit trust on the part of the user. As users are habituated to the presence of voice-activated home assistants, they believe that the technology will act in its owner's best interest, displaying trust in the devices. Human-computer interaction experts argued that as habituated technological devices become a routine part of people's lives and provide pleasurable experiences that enhance their lives, they would become irreplaceable over time (Soro et al. 2016). Furthermore, researchers from George Mason University observed that those interacting with technology tend to be positively inclined towards them in a phenomenon known as automation bias, which results in greater faith in the ability of the technology and reduction in verification-seeking behaviour on the part of the user (de Visser et al. 2016). For home assistants like Echo, there is expectation on the part of the user that it will record only what is favourable to the users within the confines of the homes, for example.

However, the expectation that smart technology will serve only benefits while minimising any potential risk is an unrealistic one. Consequences from shifting behaviour norms range from privacy and security challenges to possible aggravation of existing social issues.

***Unintended Consequences***

Fears of voice-activated technologies overhearing more than intended may significantly impact users' behaviours towards such devices. Instances of accidental audio recordings feature prominently in the media (Bhattacharya 2017; Bradshaw 2017). For example, a smart thermostat in a user's home was reset after his Echo device responded to a radio broadcast (Smith 2016). Unintentional recording raises concerns over the erosion of privacy in users' homes, and leads to the belief that no conversation is 'safe' from such devices. The potential for unintentional recordings of sensitive information such as passwords and personal indiscretions may potentially reduce trust in these devices (Lewis 2016).

Concern about unintended recordings largely stems from the speech-activated devices' built-in microphones, which monitor the environment for voice command to activate recording (Gray 2016). This is further amplified by audio sensors on these devices which are capable of hearing voices from across a room. Users may become self-conscious around these devices and alter their behaviours in conversations to reduce fears or suspicions of unwanted eavesdropping. There have also been instances of these devices misinterpreting certain voices as their wake word and performing unintended tasks. For example, Google Home falsely recognised a voiceover on a Burger King advertisement as a user query to define a Whopper burger, allowing opportunists to make a sales pitch for the burger in the process (Kastrenakes 2017).

***Intentional Exploitation***

Speech-activated technology may be exploited. Home assistants may be deliberately turned into device for espionage purposes. On 7 March 2017, Wikileaks

revealed the CIA's global covert hacking program against a wide range of American and European technological products such as Apple's iPhones, Google's Android, Microsoft's Windows and Samsung TVs, which are turned into covert microphones (Wikileaks 2017) In 'fake-off' mode, the device in fact stays 'on', recording conversations in the room and sending them over the internet to a covert CIA server (Wikileaks 2017). It is thus conceivable that home assistants like Echo, which already have microphone built into the devices, will or may in fact have become part of the arsenal for espionage in future.

Technology companies like Amazon and Google have taken security measures against the threat of surveillance, encrypting audio that is transferred from user homes into the companies' data centres (Moynihan 2016). While the companies may succeed in assuring consumers of the privacy of their data, given the cat-and-mouse game of international espionage, it is uncertain how long these measures will go in ensuring privacy and security. Furthermore, experts have cautioned that it is far more likely that criminals obtain device passwords and access users' history logs (Moynihan 2016). Security-related implications of speech-activated devices will thus be an ongoing challenge in future.

## DISCUSSION AND CONCLUSION

Smart technology invariably poses challenges to user privacy and personal data (White House 2014). The tendency for companies to beat competitors in meeting market demands, however, meant that technology is frequently pushed out to the market quickly while failing to take into account potential risks. Korean technology giant Samsung, for instance, was compelled to release a statement clarifying that their smart TVs' voice recognition system is only activated upon clicking on a remote control button after the devices were accused of monitoring user conversations (Samsung Newsroom 2015). While users respond enthusiastically to new technology, they also need firm assurance that their devices will work for them, not against them. This mind-set is behind the murder case involving Amazon Echo, where the U.S. Fourth Amendment had been invoked to protect the suspect from providing data from the device to the prosecutors (Buhr 2016). The Fourth Amendment, which is enshrined in the U.S. constitution, aims to protect individuals' right to be 'secure in their persons, houses, papers, and effects' against unreasonable intrusions by the US government (Kim 2017). The late Supreme Court Justice Anthony Scalia pointed out that the Fourth Amendment "…draws a firm line at the entrance to the house" (Supreme Court of the United States 2001), highlighting the extent to which the privacy and sanctity of a home is respected (Jerome 2017). The home is thus a protected entity under legislation like the Fourth Amendment. However, with the introduction of the third party doctrine, where information that is shared with outside parties loses its private status, it becomes increasingly challenging to apply the principle of the sanctity of the home (Gray 2016). With Internet-of-Things (IoT) devices like speech-activated home assistants increasingly comprising part of smart homes (Taylor 2007), the challenge is exacerbated. Certainly the Amazon case was a weak one, given the lawful subpoena provided by law enforcement and the fact that the suspect's reasonable expectation of

privacy has been given up to the third-party of Amazon (Gray 2016; Heater 2017). While some providers of speech-activated devices (e.g. Amazon) enable users to review and delete device recordings, the third-party doctrine overrides any confidentiality clause (Jerome 2017). The doctrine also applies in spite of the duration the recording is held for (Jerome 2017). What is clear from the Amazon Echo case is that it will not be the last time that the right to user privacy is invoked in future legal cases involving speech-activated technology.

For practitioners, this meant that legal provision must be made to accommodate potentially ubiquitous technology. Currently, speech-activated home assistants do not fall into the purview of existing legislation. For instance, South Korea's Act on the Promotion of Information Communication Network Utilisation and Information Protection (PICNUIA), which requires information service providers to seek prior consent from users to access personal data (Kwang and Ju 2017), is oriented towards regulating smartphone. Even in the U.S., where the market for speech-activated home assistant is, the United States Congress has yet to put in place safeguards and guidelines for speech-activated devices (Stanley 2017). Thus legislative provision with specific standards outlining when and how governments and corporations can access data from speech-activated home assistants must be drawn. For technology companies, the above discussion means that the onus is on them to adhere to ethics when considering technological design and potential challenges that will be faced during implementation. There is a need to safeguard consumer privacy through providing clear visual cues that indicate when the device is recording or transmitting information, for example (Gray 2016). As an illustration, a ring on the top of the Echo is designed to turn blue to clearly indicate the process of audio recording for users (Steele 2016). Research and development should also consider, as far as possible, vulnerabilities in terms of shifting behavioural norms as a result of usage of speech-activated technologies. While safeguarding user privacy is an important part of retaining trust in the technology, other ethical considerations that affect the society as a whole must be considered: what happens to the data in the event of criminal exploitation? How should the cooperation with law enforcement and other security services take shape? The fact that the functions of home assistants are evolving, becoming phones, for example, and is now able to control other devices (Welch et al. 2017; Wong 2017), meant that other challenges will come to the fore in time. Thus technology companies must consider ethics when it comes to technological design.

Meanwhile, the future seems set to be an interesting one for speech-activated technology. The functions of home assistants, for example, are evolving. Google Home is now becoming phones, for example, and is also able to control other devices (Welch et al. 2017; Wong 2017). Home assistants like Apple's newly launched HomePod, for example, have every potential to become future 'smart home hub' (Creighton 2017). Given the fact that speech-activated home assistants are slowly but surely turning into part of the Internet-of-Things (IoTs), these devices may in time become part of the solution for security (Tan 2016). For instance, Scout is a device that connects to Amazon Echo through a hub and has an array of motion sensors and access detectors (Amazon 2017d). Users can arm home alarms, call for help, trigger sirens and set pre-

programmed modes using this device (Wollerton, 2016). As functions of speech-activated technology increase, the prospect of mass adoption is likely to rise as well.

On a wider scale, emotional reliance on smart home assistant may exacerbate social issues in future. For example, Japanese technology company Vinclu targets its Gatebox Communication Robot at the country's single population, which has become the largest segment of the population at 32.5 percent out of 51.88 million households in 2015 (Ryall 2016). Gatebox's holographic home assistant, Azuma Hikari wakes her 'master' up every morning, sends him text messages, reminds him to bring umbrella and ensures that the light and heating are switched on before he reaches home, fulfilling the company's aim of being 'naturally in [their] daily lives' (Ryall 2016). If widely adopted, home devices like Gatebox can become such effective companions to the single population that they see no need for real-life human companion, further exacerbating the challenges of falling birth rate in the country. Already, debates over conferring personhood status to ambient technology like robots have begun in Japan (Robertson 2014) and the European Union (EU) (CNBC 2016). The fact that these debates exist reveal a potentially troubling future whereby emotional reliance on intelligent technology replaces trust in other humans. Future policies need to address the question of whether the companionship brought about by home assistants ironically lead to increasing isolation and thereby contribute to problems in the society.

Furthermore, in the future where speech-activated technology becomes increasingly prevalent, social cleavages may become exacerbated. For example, ownership of smart home assistants like Echo and Home may in future signal social status in the same way that being able to employ a butler is an indication of wealth in some parts of the world today. Also, early adopters of speech-activated devices may gain distinct advantages over late adopters and those who do not have access to these devices, such as faster access to knowledge and more efficient time management. While speech-activated technology presents a myriad of possibilities, it can also exacerbate social differences between individuals and groups.

However, the question remains as to whether concern for privacy will hamper the mass adoption of speech-activated technology? For now, despite advances in speech recognition, most users continue to swipe, tap and click (Cao and Bass 2016), behaviours which preserve privacy better than voicing command out loud. Research towards incorporating non-audible inputs, such as gesture recognition for example, is already ongoing. A study by Juniper Research predicted that by the end of 2016, there will be roughly 168 million devices including wearables that utilise motion or gesture tracking (Pierson 2016). Microsoft's gesture recognition research project allows users to prod a stuffed rabbit, turn a knob or switch a dial on screen (Linn 2016). These technological developments all represent competition to possible disruptive effect of speech-activated technology. Therefore, concern for privacy may ironically prevent speech-activated technology from becoming ubiquitous in the first place.

## REFERENCES

Amazon. "Customer Reviews: Amazon Echo Black". Accessed June 02, 2017a. https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa/product-reviews/B00X4WHP5E

Amazon. "Echo and Alexa Devices". Accessed June 06, 2017b. https://www.amazon.com/Amazon-Echo-And-Alexa-Devices/b?ie=UTF8&node=9818047011

Amazon. "Introducing Echo Show". Accessed June 07, 2017c. https://www.amazon.com/Amazon-MW46WB-Introducing-Echo-Show/dp/B01J24C0TI

Amazon. "Scout Alarm Wireless Motion Sensor, Arctic". Accessed June 06, 2017d. https://www.amazon.com/Scout-Alarm-Wireless-Motion-Sensor/dp/B00HC1CNXM

Apple. "World Wide Developer Conference 2017". Accessed June 06, 2017. https://developer.apple.com/wwdc/

Bhagat, Rahil. "Living with the Amazon Echo is More Challenging Than We Thought", *Stuff*, 23 February, 2016. Accessed June 06, 2017. https://www.stuff.tv/sg/features/living-amazon-echo-more-challenging-we-thought

Bhattacharya, Ananya. "Amazon's Alexa Accidentally Ordered A Ton of Dollhouse Across San Diego". *Quartz*, January 07, 2017. Accessed June 01, 2017. https://qz.com/880541/amazons-amzn-alexa-accidentally-ordered-a-ton-of-dollhouses-across-san-diego/

Bowles, Nellie. "'She Has a Name': Amazon's Alexa is a sleeper hit, with serious superfans". *The Guardian*, April 26, 2016. Accessed June 02, 2017. https://www.theguardian.com/technology/2016/apr/26/amazon-echo-alexa-voice-recognition-superfans

Bradshaw, Tim. "Burger King Activates a Google Home Controversy". *Financial Times*, April 13, 2017. Accessed May 31. https://www.ft.com/content/480e5ba6-202b-11e7-a454-ab04428977f9

Buhr, Sarah. "An Amazon Echo May be the Key to Solving a Murder Case". *TechCrunch*, December 27, 2016. Accessed May 26, 2017. https://techcrunch.com/2016/12/27/an-amazon-echo-may-be-the-key-to-solving-a-murder-case/

Busatlic, Bekir, Nejdet Dogru, Isaac Lera, and Enes Sukic. "Smart Homes with Voice Activated Systems for Disabled People". *TEM Journal* 6 (2017): 103-107. doi: 10.18421/TEM61-15.

Calore, Michael. “Watch People with Accents Confuse the Hell out of AI Assistants”. *WIRED*, May 16, 2017. Accessed May 29. https://www.wired.com/2017/05/ai-assistants-accented-english/

Canny, John. “The Future of Human-Computer Interaction: Is an HCI revolution just around the corner?”. *ACM Queue* 4 (2006): 26-32. http://queue.acm.org/detail.cfm?id=1147530

Cao, Jing and Dina Bass. “Speech Recognition Must Get Much Better If We Are to Speak Naturally to Our Gadgets. So the Tech Industry is Vacuuming Up all the Conversations It Can.” *Bloomberg Technology*, December 13, 2016. Accessed June 05, 2017. https://www.bloomberg.com/news/articles/2016-12-13/why-google-microsoft-and-amazon-love-the-sound-of-your-voice

Creighton, Jolene. “Apple Just Unveiled a Breakthrough Artificial Intelligence System”, *Futurism*, June 06, 2017. Accessed June 06. https://futurism.com/apple-just-unveiled-a-breakthrough-artificial-intelligence-system/

Department of Statistics Singapore. “Population Trends 2016”. Accessed May 30, 2017. http://www.singstat.gov.sg/docs/default-source/default-document-library/publications/publications_and_papers/population_and_population_structure/population2016.pdf

de Visser, Ewart, Samuel S Monfort, Ryan Mckendrick, Melissa A. B. Smith, Patrick Mcknight, Frank Krueger, Raja Parasuraman. “Almost Human: Anthropomorphism Increases Trust Resilience in Cognitive Agents.” *Journal of Experimental Psychology: Applied* 22 (2016): 331-349.

Duran, Michael. “How to Set Up Your New Amazon Echo”. *Wired*, December 25, 2016. Accessed June 06, 2017. https://www.wired.com/2016/12/set-new-amazon-echo/

Elwood, Susan A. “Embedding Ubiquitous Technologies”. In *Encyclopedia of Information Technology Curriculum Integration*, edited by Tomei, Lawrence A., 279-285. Hershey, PA and London: Information Science Reference, 2008.

Fitzsimmons, Michelle. “Google IO 2016: All the News from Google's Huge Event”. *Techradar.com*, May 20, 2016. Accessed September 16. http://www.techradar.com/news/world-of-tech/google-io-1307820

Galeon, Dom. “Microsoft’s Speech Recognition Tech is Officially as Accurate as Humans”. *Futurism*, October 21, 2016. Accessed October 21. http://futurism.com/microsofts-speech-recognition-tech-is-officially-as-accurate-as-humans/

Gartner. “Gartner Says by 2019, 20 Percent of User Interactions with Smartphones Will Take Place via VPAs”. Accessed December 21, 2016. http://www.gartner.com/newsroom/id/3551217

Google. “Google I/O 2016”. Accessed June 06, 2016. https://events.google.com/io2016/

Google. “Google I/O 2017”. Accessed June 06, 2017. https://events.google.com/io/

Gray P., Hovav A. “Methods for Studying the Information Systems Future”. In: *Researching the Future in Information Systems*, edited by Chiasson M., Henfridsson O., Karsten H., DeGross J.I., 327-346. Berlin and Heidelberg: Springer, 2011.

Gray, Stacey. “Always On: Privacy Implications of Microphone-Enabled Devices”. *Future of Privacy Forum*, April, 2016.

Guye-Vuillème, Anthony, Tolga K. Capin, S. Pandzic, N. Magnenat Thalmann, and Daniel Thalmann. “Nonverbal Communication Interface for Collaborative Virtual Environments”, *Virtual Reality* 4 (1999): 49–59. Accessed June 06, 2017. https://link.springer.com/article/10.1007/BF01434994

Hagsall, Alon A. “From Assimilation to Acclimatization of Social Digital Technology in Organizations”. *International Journal of Computer Systems* 02 (2015): 405-410.

Hamilton, Laura. “What Is Voice Control’s Role in Driving Smart Home Technology Adoption?”. *CED Magazine*, April 11, 2016. Accessed June 02, 2017. https://www.cedmagazine.com/data-focus/2016/11/what-voice-controls-role-driving-smart-home-technology-adoption

Heater, Brian. “Can Your Smart Home be Used Against You in Court?”. *TechCrunch*, March 12, 2017. Accessed June 05, 2017.https://techcrunch.com/2017/03/12/alexa-privacy/

“How Voice Technology is Transforming Computing”. *The Economist*, January 07, 2017. Accessed June 01, 2017. http://www.economist.com/news/leaders/21713836-casting-magic-spell-it-lets-people-control-world-through-words-alone-how-voice

Jerome, Joseph. “Alexa, Is Law Enforcement Listening?”. *Center for Democracy and Technology*, January 04, 2017. Accessed May 30. https://cdt.org/blog/alexa-is-law-enforcement-listening/

Kahneman, Daniel. *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux, 2011.

Kastrenakes, Jacob. “Burger King’s New Ad Forces Google Home to Advertise the Whopper”. *The Verge*, April 12, 2017. Accessed June 07, 2017. https://www.theverge.com/2017/4/12/15259400/burger-king-google-home-ad-wikipedia

Kim, Jonathan. “Fourth Amendment”, *Cornell University Law School Legal Information Institute*, June 1, 2017. Accessed July 20, 2017. https://www.law.cornell.edu/wex/fourth_amendment

Klofstad, Casey A, Stephen Nowicki, and Rindy C. Anderson. "How Voice Pitch Influences Our Choice of Leaders". *American Scientist*, September – November Issue (2016). Accessed June 04, 2017. http://www.americanscientist.org/issues/feature/2016/5/how-voice-pitch-influences-our-choice-of-leaders/1

Kwang, Bae Park, and Bong Jang Ju. "South Korea: Act on Promotion of Information and Communications Network Utilization and Information Protection and The Personal Information Protection Act Amended", *Mondaq,* January 25, 2017. Accessed July 21, 2017. http://www.mondaq.com/x/562942/Data+Protection+Privacy/Act+On+Promotion+Of+Information+And+Communications+Network+Utilization+And+Information+Protection+And+The+Personal+Information+Protection+Act+Amended

Lewis, David. "Think Before You Speak: Voice Recognition Replacing the Password". *Information-Age.com*, August 01, 2016. Accessed June 01, 2017. http://www.information-age.com/think-you-speak-voice-recognition-replacing-password-123461752/

Levithin, Daniel J. *The Organised Mind: Thinking Straight in the Age of Information Overload*. New York: Dutton, 2014.

Li, Gong, and Jennifer Lai. "Shall We Mix Synthetic Speech and Human Speech?". *Stanford University*, March 01, 2001. Accessed June 04, 2017. http://www.csis.pace.edu/~ctappert/dps/pdf/lai/mix.pdf

Linn, Allison. "Talking with Your Hands: How Microsoft Researchers Are Moving Beyond Keyboard and Mouse". *Microsoft Blog*, June 26, 2016. Accessed December 07, 2016. http://blogs.microsoft.com/next/2016/06/26/talking-hands-microsoft-researchers-moving-beyond-keyboard-mouse/#HBA9v3cWOLKX9FgY.99

Milanesi, Carolina. "Should Virtual Assistants be Humanised?". *TechPinions*, May 25, 2016. Accessed June 03, 2017. https://techpinions.com/should-virtual-assistants-be-humanized/45809

Mims, Christopher. "Your Next Friend Could Be A Robot". *The Wall Street Journal*, October 09, 2016. Accessed May 31, 2017. https://www.wsj.com/articles/your-next-friend-could-be-a-robot-1476034599

Mitchell, Wade J, Kevin A Szerszen, Sr, Amy Shirong Lu, Paul W Schermerhorn, Matthias Scheutz, and Karl F MacDorman. "A Mismatch in the Human Realism of Face and Voice Produces an Uncanny Valley", *i-Perception* 2 (2011): 10 – 12. http://www.macdorman.com/kfm/writings/pubs/Mitchell2011HumanRealismMismatch.pdf

Moynihan, Tim. "Alexa and Google Home Record What You Say. But What Happens to That Data?" *WIRED*, May 12 (2016). Accessed June 02, 2017. https://www.wired.com/2016/12/alexa-and-google-record-your-voice/

Nelson, Patrick. “Adoption of Voice-first Assistants Expected to Skyrocket”. *Network Wordl,* March 15 (2017). http://www.networkworld.com/article/3181313/software/adoption-of-voice-first-assistants-expected-to-skyrocket.html

WIRED Staff. “OK, House. Get Smart: Make the Most of Your AI Home Minions”.. *WIRED,* May 16, 2017. Accessed 4 June 2017. https://www.wired.com/2017/06/guide-to-ai-artificial-intelligence-at-home?mbid=nl_6317_p1&CNDID=43852638

Pardes, Arielle. “Everything Apple Announced Today at WWDC”. *WIRED*, June 05, 2017. Accessed June 06, 2017. https://www.wired.com/2017/06/everything-apple-announced-today-wwdc/?mbid=nl_6517_p10&CNDID=43852638

Payne, Jeunese A, Graham I. Johnson, and Andrea Szymkowiak. “The Behavioural Impact of a Visually Represented Virtual Assistant in a Self-Service Checkout Context”. In Proceedings of the 25th BCS Conference on Human-Computer Interaction, 58-63, 2011. British Computer Society.

Paul, Aaron. “Can Amazon’s Alexa Be Your Friend?”. *Digg*, March 30, 2017. Accessed June 03, 2017. http://digg.com/2017/amazon-alexa-is-not-your-friend

Perez, Sarah. “’Elderly Alexa’ Helps Families Care for Their Remote Loved Ones via Voice”. *TechCrunch*, May 14, 2017. Accessed June 06, 2017. https://techcrunch.com/2017/05/14/elderly-alexa-helps-family-care-for-their-remote-loved-ones-via-voice/

Pierson, Ryan Matthew. “Study Suggests a Half-billion Gesture-tracking Devices by 2021.” *Readwrite*, November 07, 2016. Accessed November 21, 2016. http://readwrite.com/2016/11/07/study-suggests-500-million-motion-and-gesture-tracking-devices-by-2021-dl4/

Qiu, Lingyun and Izak Benbasat. 2009. “Evaluating Anthropomorphic Product Recommendation Agents: A Social Relationship Perspective to Designing Information Systems”. *Journal of Management Information Systems* 25 (2009): 145-182. doi: 10.2753/MIS0742-1222250405

Ramakrishnan, S. and Ibrahiem M.M. El Emary. “Speech Emotion Recognition Approaches in Human Computer Interaction”. *Telecommunication System* 52 (2012): 1467-1478.

Robertson, Jennifer. “Human Rights vs. Robot Rights: Forecasts from Japan”. *Critical Asian Studies* 46 (2014): 571-598.

CNBC. “Robots Could Become 'Electronic Persons' with Rights, Obligations under Draft EU Plan”. *CNBC*, June 21, 2016. Accessed June 07, 2017. http://www.cnbc.com/2016/06/21/robots-could-become-electronic-persons-with-rights-obligations-under-draft-eu-plan.html

Rosenwald, Michael S. "How Millions of Kids Are Being Shaped by Know-it-all Voice Assistants". *The Washington Post*, March 01, 2017. Accessed June 03, 2017. https://www.washingtonpost.com/local/how-millions-of-kids-are-being-shaped-by-know-it-all-voice-assistants/2017/03/01/c0a644c4-ef1c-11e6-b4ff-ac2cf509efe5_story.html?utm_term=.d811513de9df

Ryall, Julian. "Holographic 'Wife' Ministers to Japan's Single Men". *The Telegraph*, December 16, 2016. Accessed May 26, 2017. http://www.telegraph.co.uk/news/2016/12/16/holographic-wife-ministers-japans-single-men/

Samsung Newsroom. "Samsung Smart TVs Do Not Monitor Living Room Conversations". February 10, 2015. Accessed June 05, 2017. https://news.samsung.com/global/samsung-smart-tvs-do-not-monitor-living-room-conversations

Service, Owain, Michael Hallsworth, David Halpern, Felicity Algate, Rory Gallagher, Sam Nguyen, Simon Ruda, Michael Sanders. "EAST: Four Simple Ways to Apply Behavioural Insights", *The Behavioural Insights Team*, April 11, 2014. Accessed June 06, 2017. http://www.behaviouralinsights.co.uk/publications/east-four-simple-ways-to-apply-behavioural-insights/

Singularity Lectures. "Andrew Ng - Deep Learning in Practice: Speech Recognition and Beyond". 2016. *Singularity Lectures*, May 23, 2016. Accessed November 17. https://www.youtube.com/watch?v=LFDU2GX4AqM

Smith, Chris. "Radio Broadcast Caused Amazon Echo to Reset User's Home Thermostat". *Trusted Reviews*, March 11, 2016. Accessed June 07, 2017. http://www.trustedreviews.com/news/radio-broadcast-caused-amazon-echo-to-reset-user-s-home-thermostat#8IPemaDJPAz0xGKd.99

Soro, Alessandro, Margot Brereton, and Paul Roe. "Towards an Analysis Framework of Technology Habituation by Older Users." Paper presented at the *2016 ACM Conference on Designing Interactive Systems*, Brisbane, Australia, June 04-08, 2016.

Stanley, Jay. "The Privacy Threat from Always-On Microphones Like the Amazon Echo". *American Civil Liberties Union*, January 13, 2017. Accessed May 31, 2017. https://www.aclu.org/blog/free-future/privacy-threat-always-microphones-amazon-echo

Steele, Billy. "Police seek Amazon Echo data in murder case (updated)". *Engadge*t, December 27, 2016. Accessed June 05, 2017. https://www.engadget.com/2016/12/27/amazon-echo-audio-data-murder-case/

Stern, Joanna. "Alexa, Siri, Cortana: The Problem with All-Female Digital Assistants". *The Wall Street Journal*, February 21, 2017. Accessed June 04, 2017.

https://www.wsj.com/articles/alexa-siri-cortana-the-problem-with-all-female-digital-assistants-1487709068

Stinson, Lisa. "The Surprising Repercussions of Making AI Assistants Sound Human". *WIRED*, May 12, 2017. Accessed June 04, 2017. https://www.wired.com/2017/05/surprising-repercussions-making-ai-assistants-sound-human/?utm_source=MIT+Technology+Review&utm_campaign=eddf531469-The_Download&utm_medium=email&utm_term=0_997ed6f472-eddf531469-154825137

Sullivan, Mark. "The Real Reasons that Amazon's Alexa May Become the Go-To AI For The Home". *Fast Company*, August 04, 2016. Accessed June 05, 2017. https://www.fastcompany.com/3058721/the-real-reasons-that-amazons-alexa-may-become-the-go-to-ai-for-the-home

Supreme Court of the United States. "Kyllo v. United States". *Cornell University Law School Legal Information Institute*, June 11, 2001. Accessed June 21, 2017. https://www.law.cornell.edu/supct/html/99-8508.ZS.html

Talbot, David. "The Era of Ubiquitous Listening Dawns". *MIT Technology Review*, August 08, 2013. Accessed May 30, 2017. https://www.technologyreview.com/s/517801/the-era-of-ubiquitous-listening-dawns/

Tan Teck Boon. "Pitfalls of the 'Internet-of-Things'". *RSIS Commentary*, 13 June, 2016.

Taylor, Alex S., Richard Harper, Laurel Swan, Shahram Izadi, Abigail Sellen, and Mark Perry. "Homes that Make Us Smart". *Pers Ubiquit Comput* 11 (2007): 383–393. doi: 10.1007/s00779-006-0076-5.

White House. "Big Data and Privacy: A Technological Perspective", The White House President's Council of Advisors on Science and Technology, May, 2014. Accessed June 03, 2017. https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf

Transparency Market Research. "Growing Focus on Strengthening Customer Relations Spurs Adoption of Intelligent Virtual Assistant Technology, says TMR", *Transparency Market Research*, August 02, 2016. Accessed June 06. http://www.transparencymarketresearch.com/pressrelease/intelligent-virtual-assistant-industry.htm

Waters, Richard. "Ford Enlists Amazon's Alexa as Driver Assistant". *Financial Times*, January 05, 2017. Accessed June 03. https://www.ft.com/content/fd94edca-d2fe-11e6-9341-7393bb2e1b51

Welch, Chris, Sean O'Kane, and Nick Statt. 2017. "The 10 Biggest Announcements From Google I/O 2017". *The Verge*, May 17. Accessed May 26, 2017.

https://www.theverge.com/2017/5/17/15654432/google-io-2017-keynote-highlights-news-announcements-recap

Wikileaks. "Vault 7: CIA Hacking Tools Revealed". Accessed May 04, 2017. https://wikileaks.org/ciav7p1/

Wollerton, Megan. "Scouting Out a Security System That Talks to Amazon's Alexa". *CNET*, March 16, 2016. Accessed June 04, 2017. https://www.cnet.com/news/scouting-out-a-security-system-that-talks-to-amazons-alexa/

Wong, Raymond. "Thanks to Amazon, It's Time to Kill Your Landline". *Mashable Asia*, May 10, 2017. Accessed 02 June 2017. http://mashable.com/2017/05/09/amazon-echo-calling-landline-replacement/#FlxMzgjWmmqw

Townsend, Tess. "Google Home Can Now Recognize Different Users by Their Voice". *Recode*, April 20, 2017. Accessed May 31. https://www.recode.net/2017/4/20/15364120/google-home-multiple-accounts

Zoughbi, Saleem and Sukaina Al-Nasrawi. "Regional Development Getting Smarter with ICT". In *Encyclopaedia of Information Science and Technology, Third Edition*, ed. Khosrow-Pour, Mehdi, 6525-6533. Hershey, PA: Information Science Reference, 2015

RESEARCH ARTICLE

# Exploring a New Approach to Business Continuity Management Training Practices by Singapore Hotels to Manage Terrorist Threats

***Kevin Thian Hock Wee***[1]

AJPA Asian Journal of Public Affairs

**Keywords**: Hotels, training, Business Continuity Management, Computer simulation games, terrorist threats

**Suggested Article Citation**: Wee, Kevin. 2017. "Exploring a New Approach to Business Continuity Management Training Practices by Singapore Hotels to Manage Terrorist Threats." *Asian Journal of Public Affairs* 10(1): p.85-102

http://dx.doi.org/10.18003/ajpa.2017312

ISSN 1793-5342 (print); ISSN 2382-6134 (online),  Published by Lee Kuan Yew School of Public Policy, National University of Singapore

**ABSTRACT**

*Singapore is vulnerable to terrorist threats. This reality was reinforced by terrorist attacks in South East Asia in recent years of. Attacks on soft targets by self-radicalized "lone-wolves" add a new dimension as these are difficult to prevent. Hotels are most vulnerable as they remain accessible to the general public. The Singapore Government has involved the private sector to help counter terror threats. Private sector companies should therefore adopt Business Continuity Management (BCM) systems and train their staff to take on this role. This paper reviews the current BCM and training practices of Singapore hotels. The findings reveal that most hotels have BCM systems and virtually all security staff and crisis team members undergo anti-terrorism training. However, many BCM systems are not based on industry standards and the majority of hotel employees are not trained. Computer simulation games could be a step to address some of these issues.*

## INTRODUCTION

The threat of terror attacks affects cities around the world, including Singapore. The recent Terrorism Threat Assessment Report (Ministry of Home Affairs, 2017) revealed that the threat is "the highest in recent years" evidenced by attacks in Indonesia and Malaysia in 2016 and the siege of Marawi City in the Philippines in May 2017. Besides bombing, shooting and commando-style attacks; the threat has evolved

[1] Kevin Wee is a Senior Lecturer in the School of Business Management, Nanyang Polytechnic, Singapore. Email: kevin_wee@nyp.edu.sg

to include attacks by self-radicalized "lone-wolves" using everyday items as weapons, as demonstrated in the London Bridge attacks in June 2017. Such plots are difficult to detect and prevent as they can be planned without leaving any obvious traces.

Terrorists have attacked public venues, i.e. "soft targets", such as airports, retail malls, entertainment venues, and hotels. It is impossible to fortify every potential target. Government agencies and private sector security professionals must therefore strike a balance between protection and accessibility. Hotels, by nature of the service that they provide, are particularly vulnerable (Harwood, 2009) and have suffered a series of attacks that include the 2008 Mumbai (India) attacks on the Taj Mahal Palace Hotel and Trident-Oberoi, the 2009 bomb attacks on the JW Marriott and Ritz-Carlton Hotels in Jakarta (Indonesia), and the 2015 attack on the Soviva and Imperial Marhaba hotels in Sousse (Tunisia).

Hotel managers cannot employ common security measures found in office buildings or industrial properties such as requiring guests to display security passes. They have to develop effective solutions to address this threat. This is a challenge as the terrorists can adapt their plans to combat measures implemented to destroy or hinder them (Gunaratna, 2004). The perpetrators in the Mumbai attacks displayed a level of planning and sophistication that overwhelmed the capabilities of both government agencies and private sector security professionals for an extended period of time. The high death toll and the slow and uncoordinated government response further strengthened the impact of the attack (Tellis et al, 2009). This sophistication was again demonstrated by the attackers of the JW Marriott and Ritz-Carlton hotels in Jakarta. They eluded the security agencies (Onishi, 2009) and penetrated the security layers in place by checking in as hotel guests and smuggling the bombs through the hotel's employee entrance (Stewart, 2016). They also sought to exploit the hotel's evacuation procedures by timing a bomb in their hotel room to explode first whilst the remaining bombs were detonated when people would be evacuated through the lobby entrances (Barta and Carder, 2009).

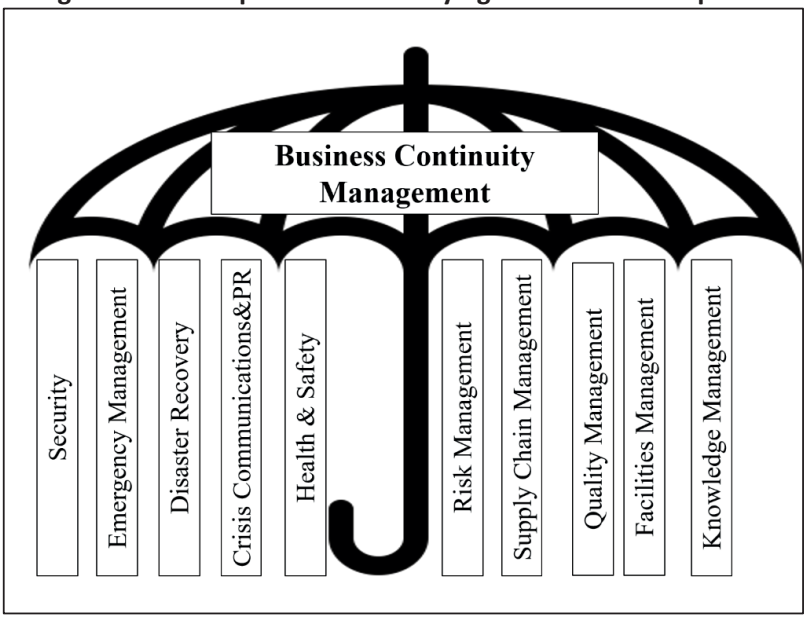
In view of these realities, the Singapore Government has involved the private sector and the community at large[2] in countering the terrorist threat (Ministry of Home Affairs, 2017). Whilst this makes sense from a public policy perspective, it is important that private sector companies adopt Business Continuity Management (BCM) systems and train their staff to take on this expanded role. The purpose of this study is to examine the current BCM and training practices that Singapore hotels have adopted to respond to crisis situations - particularly terrorist attacks. The study will also review the implications on public policies that seek to leverage on private sector resources in fighting terrorism. The possibility of using Computer simulation games as a training format for hotel employees will also be explored.

[2] The government introduced the SG Secure programme in 2016 to involve the entire population in Singapore to prevent and deal with a terrorist attack (Lee, 2016).

## BUSINESS CONTINUITY MANAGEMENT (BCM) AND CRISIS MANAGEMENT

Business Continuity Management (BCM) is defined by the Business Continuity Institute (BCI) as a "holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities". A good BCM framework unifies various disciplines (Smith, 2003) including security, emergency management, and disaster recovery (Figure 1).

**Figure 1: The Scope of BCM – Unifying the Various Disciplines**

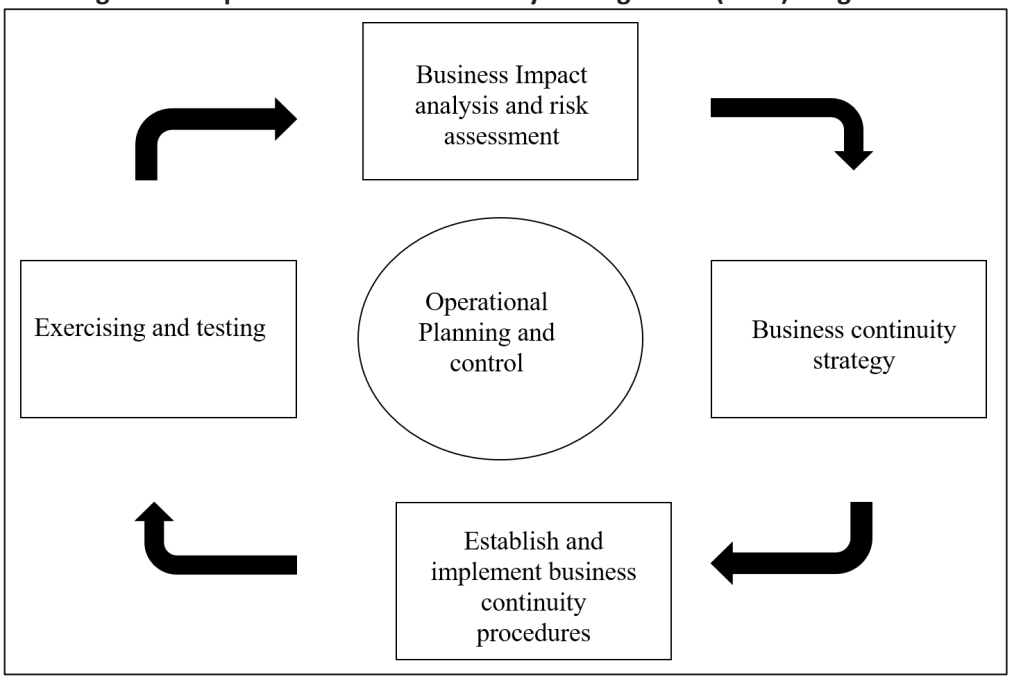



***Source:*** Adapted from David Smith. "Business continuity and crisis management." *Management Quarterly* 44, no. 1 (2003): 27-33.

The BCI also developed a set of principles – two of which are pertinent to this study. First, BCM and crisis management are integral parts of corporate governance; and second, the organization must implement and maintain a robust exercising, rehearsal, and testing programme (Smith 2003).

As in Figure 2 below, companies that adopt a BCM System will follow a few basic steps as outlined in the Singapore Standard for Societal Security 2013 (that is applicable to all companies in Singapore). Essential business activities that must remain uninterrupted during a crisis are identified via a Business Impact Analysis. Strategies and procedures are then developed and the necessary resources and training are provided to achieve this continuity.

**Figure 2: Steps in a Business Continuity Management (BCM) Programme**




***Source:*** Singapore Standards Societal security – Business Continuity Management systems – Guidance SS ISO 22313:2013

In the case of hotels, the maintenance of accurate records of in-house guests is an essential activity. Details such as check-in/check-out dates and the room assignment for all guests are stored in computer systems both on the hotel premises and at back-up locations. Hard copies are kept by the Front Desk Department that are regularly updated, kept in a secure location, and are accessible in the event of a crisis; e.g. a fire outbreak. Front Desk staff would use these to confirm the identity of guests gathered at the assembly point after an evacuation.

Staff undergoes regular training exercises, and audits are carried out to test if they comply with required standards. Adequate training helps prepare staff to manage crises effectively (McMullan and Baum, 2011). Several training formats are commonly used as seen in Table 1.

**Table 1: Training Formats**

| Training Format | Description |
|---|---|
| *Guidelines and Procedures* | These serve as a repository of information and can be circulated quickly to other staff via email or through the usual means of staff communication. |
| *Classroom Exercises* | These are used to introduce new procedures to existing staff or to acquaint new staff with existing practices in a classroom setting. Staff can apply their knowledge through case studies and clarify their |

| | |
|---|---|
| | doubts via question and answer sessions. These have limited impact on business operations as they are scheduled in advance and trainees can arrange for other staff to cover their duties. |
| *Table-Top Exercises* | These are used to test participants on their responses to crisis scenarios using existing BCM procedures and plans. Staff form small groups and discuss questions presented to them by a facilitator in a workshop format. At the end of the exercise, the facilitator will review and discuss any deviations from procedures and explore ways to improve the responses. These exercises require a significant amount of time from the crisis management team and selected members from senior management. |
| *Drills and Full Scale Exercises* | These are the costliest in terms of time commitment and disrupt the company's normal business operations which are usually suspended during the exercise. Almost all staff may be involved. These feature realistic scenarios and require participants to implement procedures as if an actual crisis was occurring. |

***Source:*** Adapted from Kurt J Engemann and Douglas M. Henderson. *Business Continuity and Risk Management: Essentials of Organizational Resilience.* Rothstein Publishing, 2011

Computer simulation games (or Serious Games) have been included as part of the training repertoire (Susi et al., 2007). These are designed and programmed to simulate emergency scenarios where players learn, practise, and test their knowledge of crisis management procedures. They can be used to train employees in situations that are impractical or too costly to conduct; such as the evacuation from an airplane that has crashed (Chittaro, 2016) or a burning cruise ship (Strohschneider and Jürgen, 2004). Participants who were trained to evacuate an aircraft using Computer simulation games have shown better results compared to traditional tools, for instance an Aircraft Safety Card. In addition, participants who were trained using the computer games demonstrated a greater sense of control of outcomes compared to those who were not (Chittaro, 2016). Business operations can continue as per normal as staff can be scheduled for training sessions at appropriate times. Even though the financial cost to developing and utilising such exercises can be significant as this includes the cost of design, programming, hosting, and execution of the computer simulation exercises; ideally, companies should utilise all forms of training formats.

## THE SINGAPORE HOTEL INDUSTRY AND THE TERRORIST THREAT

Singapore hotels have dealt with crises such as the collapse of the Hotel New World in 1986, fires at the East Village Hotel in 2012, and the Broadway Hotel in 2015. Prior to the 9/11 attacks in New York City, hoteliers focused on crime prevention within their properties as the terrorism threat was not as pressing as it is now. Two notable cases include the 1994 incident when two Japanese tourists were attacked in their hotel room that resulted in one death (Straits Times, 1994) and the "Body parts Murder" where a tourist from the United Kingdom murdered and dismembered his roommate (Straits Times, 1995). In response to these incidents, the hotel industry collaborated with Singapore's National Crime Prevention Council (NCPC) and the Singapore Police Force (SPF) to introduce two initiatives in 1996, which are the *Hotel*

*Security Awards* (which are still on-going) that are presented to hotels with security systems that meet requisite standards, and the *Hotel Security Charter* that set minimum industry norms for security in hotels (Ho, 1996).

Shortly after the 9/11 terrorist attacks, the Singapore government foiled a terrorist plot by a regional Islamic militant group Jemaah Islamiyah (JI) that targeted the embassies of Australia, Israel, the United Kingdom, and the United States. The JI also targeted companies and locations frequented by nationals from the United States (Ministry of Home Affairs, 2003). As a result, the Singapore Hotel Association (SHA)[3] worked with the NCPC and SPF to develop a Hotel Security Manual in 2003 that provided guidance to member hotels to cope with the terrorist threat.

Asian hoteliers were reminded of the serious threat that terrorism posed with the Mumbai attacks in November 2008 and the Jakarta attacks in July 2009. In response, Singapore hoteliers worked with Singapore's standardisation authority, and unveiled the Singapore Standard for Hotel Security SS 545:2009 (2015) in 2009. This document prescribes best practices in threat assessment, security equipment, training, and procedures relating to security, emergencies and crisis response. However, the exact type of training programmes hotels must undertake are not specified in the Standard.

## PUBLIC-PRIVATE COLLABORATION IN COUNTER-TERORISM EFFORTS

At the time of writing this paper, Singapore has been spared from a terrorist attack. However, the government has repeatedly warned that it is a matter of time when a successful attack occurs in Singapore (Today, 2016). The government has provided the necessary resources, networks, and infrastructure to counter terrorist attacks. In 1999, the National Security Secretariat (NSS) was established within the Ministry of Defense to strengthen the coordination between Singapore's security agencies. In 2004, the NSS was renamed as the National Security Coordination Secretariat (NSCS) and placed under the auspices of the Prime Minister's Office to oversee and strengthen coordination across the defense, security, rescue, and intelligence agencies[4].

The NSCS is also responsible for educating the public and has released publications and videos highlighting the security threats that Singapore faces from terrorism. It organizes the National Security Conferences together with the Singapore Business Federation to educate the business community on the latest security trends.

The government has recognised the vital role played by the private sector in keeping Singapore safe, and released a set of voluntary building guidelines in 2005

[3] SHA is the umbrella body for hotels in Singapore with 150 members accounting for more than 90 percent of total gazetted room count in Singapore.

[4] National Security Coordinating Structure, *NSCS* (accessed June 05, 2017). http://www.nscs.gov.sg/public/content.aspx?sid=23.

(Building and Construction Authority et al, 2005) that advised developers, designers, and contractors on a series of practical and cost effective security measures and building design considerations to better secure their buildings. This was revised into a set of guidelines (Homefront Security Division, 2010). These guidelines include a special section for hotels advising hotel owners on issues of deterrence, pro-active security, perimeter security, access control, the setting up of a security command and control room, and relevant emergency procedures.

In 2009, private sector participants were included in drills and exercises by government agencies. Hotels, retail malls, public transport companies, and media establishments participated in Exercise Northstar VII held in July 2009 that simulated scenarios like the 2008 Mumbai attacks (Jayakumar, 2009). Several initiatives were launched to tap on private sector resources. A *Corporate First Responder*[5] Scheme was launched and the *Safety and Security Watch Groups (SSWG)* - networks that brought public and private sector actors together – were formed to enable easy dissemination of information and advisories when required. The *Project Guardian*[6] Scheme was introduced to "encourage all commercial companies employing private security protection services to pledge their support and assist the authorities in the fight against terrorism" in the areas of evacuation, cordon support, crowd control, traffic diversion and crisis communications (Singapore Police Force, 2016). Private sector security professionals are invited to attend training workshops and participate in drills with the agencies to test their own crisis responses.

These efforts seek to build a business community in Singapore that is ready to cope with a terrorist attack. This has become even more pressing in recent years when a planned attack on Marina Bay in 2016 was foiled (Straits Times, 2016)[7]. This community of ready companies can be achieved when both public and private sectors are trained effectively to perform their respective roles. The SHA has laid a good foundation for individual hotels to develop their own training programmes by prescribing the minimum standards and procedures. However, the programmes vary in terms of scope, format, and effectiveness due to the differences in company profiles, objectives and processes.

## METHODS

I developed a survey questionnaire for this research that included open-ended questions, closed-ended questions, and questions employing Likert Scales. This comprised five main sections that included the *profile of the respondent* (such as job

[5] The Scheme allows identified security personnel from premises affected by a crisis to gain access within the security cordon to assist relevant agencies in recovery efforts and investigations.

[6] The Scheme aims to enable private security staff of the affected properties to take charge during a crisis situation before the authorities arrive. See https://www.police.gov.sg/resources/prevent-terrorism/project-guardian for more details.

[7] In the investigations that followed, the government revealed that a terrorist plotter had been offered a job as a cleaner on the resort island of Sentosa.

title of the respondent, number of staff who are assigned security or crisis management roles, number of rooms, and the type of hotel concerned i.e. if it is part of an international chain or an independent hotel). Respondents were asked on the *type of policies* they used i.e. BCM, hotel security plans, and the guidelines to enhance building security; how well these policies integrated with their operational procedures; and if their policies conformed to the relevant industry standards. Questions on the type of *Management Systems* used – e.g. Access Control, Surveillance, Security, Alarms, Communications, Crisis Information Management, Information Technology, Emergency and Evacuation – were posed, together with relevant examples to help them answer the questions accurately.

Respondents were asked to indicate the skills that employees (i.e. security staff, the crisis management team, First-Aid responders, and generic hotel employees) needed to possess; the *Training* programmes they were sent for; the training formats used (i.e. Classroom sessions, Table-Top Exercises, Drills and Exercises and Computer simulation games); and their satisfaction with the outcomes. Lastly, they were queried on their familiarity with *Computer simulation games*[8] as a training format and if they were interested to use it to train their staff on crisis management procedures.

The survey was targeted at operational and security management members from Singapore hotels. SHA assisted by sending copies of the online surveys (developed and hosted on the 'SurveyMonkey' website) to their 150 ordinary members. Copies of the survey were also sent to 42 non-member hotels. Their contacts were obtained from a comprehensive list that included all Singapore hotels maintained by the Singapore Tourism Board. Fifty-five responses were received from 39 SHA member hotels, and four from non-member hotels. Thirty-nine completed surveys were received from the SHA member hotels, while only one completed survey was received from the non-member hotels. This was excluded from the study as it was too small to be representative of the group.

## FINDINGS

### *Profile of Companies*

Most respondents (62 percent) were from hotels considered "large" i.e. having at least 300 rooms[9] (Table 2). Respondents from medium hotels (from 101 to 299 rooms) formed the next largest group (29 percent). Most of the hotels were part of hotel chains – of which 71 percent were from international hotel chains whilst 13 percent were part of local hotel chains. 63 percent of the respondents were safety and security directors/ managers and 24 percent were involved in hotel operations.

[8] Respondents were shown a video clip of a computer simulation game by Tribe Studios designed for Shopping Mall security staff as an example.

[9] The classifications of hotel size are found in the Hotels Act (Chapter 127, Section 13) Hotels Licensing Regulations [20th December 1974]

**Table 2: Profile of Respondents**

| Type of Hotel | Response Percent | Response Count |
|---|---|---|
| Part of a local hotel chain | 12.7% | 7 |
| Part of a regional hotel chain | 5.5% | 3 |
| Part of an international hotel chain | 70.9% | 39 |
| An independent hotel | 10.9% | 6 |
| **Total Count:** | | **55** |
| **Number of Rooms** | **Response Percent** | **Response Count** |
| Up to 100 rooms | 9.1% | 5 |
| From 101 rooms to 299 rooms | 29.1% | 16 |
| From 300 rooms and above | 61.8% | 34 |
| **Total Count:** | | **55** |
| **Job Description** | **Response Percent** | **Response Count** |
| Safety/Security | 63.1% | 32 |
| Rooms Division | 7.8% | 4 |
| Hotel Operations | 23.5% | 12 |
| Others | 5.9% | 3 |
| **Total Count:** | | **51** |

***Source:*** Survey conducted by author from 28 April to 30 May 2017

The respondents indicated that staff in security roles formed 8 percent of the total staff strength on average, supplemented by an additional 7 percent of staff from other departments who were included in the Crisis Management Team. The average number of staff trained in First Aid was 12 percent which is above the requirement stipulated under the Workplace Safety and Health (First Aid) Regulations of one 'First Aider' for every 150 employees.

***BCM Policies***

A majority of respondents (82 percent) acknowledged that they had a BCM policy in place (Table 3) of which only 44 percent were based on the ISO Standard ISO 22301:2012. A few respondents from large hotels belonging to an international chain acknowledged that they did not have a BCM in place. Most respondents had a security plan (96 percent), of which 60 percent were based on the relevant Singapore Standard SS545:2009 (2015) and almost all the respondents had emergency management plans (98 percent). However, only 81 percent had conducted a Business Impact Analysis (i.e. they had identified the essential business activities that must remain uninterrupted during a crisis) for their hotels. Almost all respondents had their plans integrated with business operations and enjoyed the support from senior management. Only 52 percent had adopted the suggested guidelines on building security from the Ministry of Home Affairs.

**Table 3: Types of BCM Policies and Processes Adopted**

| BCM Policies in Place | Yes | % | Yes but not based on relevant standard | % | No | % | Total |
|---|---|---|---|---|---|---|---|
| Business Continuity Management Plan | 22 | 44.0 | 19 | 38.0 | 9 | 18.0 | 50 |
| Hotel Security Plan | 30 | 60.0 | 18 | 36.0 | 2 | 4.0 | 50 |
| **BCM Processes Adopted** | **Yes** | **%** | **No** | **%** | **Unsure** | **%** | **Total** |
| Risk Analysis i.e. assess the probability of threats occurring in the hotel | 43 | 89.6 | 2 | 4.2 | 3 | 6.3 | 48 |
| Business Impact Analysis i.e. assess potential impacts of threats on the hotel and its impact on operations | 39 | 81.3 | 4 | 8.3 | 5 | 10.4 | 48 |
| Emergency Management Plan i.e. plan that defines the detailed steps to respond to crisis events | 49 | 98.0 | 0 | 0.0 | 1 | 2.0 | 50 |

***Source:*** Survey conducted by author from 28 April to 30 May 2017

### *Security Systems*

The majority of respondents (more than 90 percent) had the whole suite of systems in place (Table 4). The two most common systems found (for 98 percent respondents) were access control systems and communications systems.

### *Skills and Training*

All respondents expected their security staff to utilise Standard Operating Procedures (SOP), anti-terrorism efforts, security incident management, crowd control, and security equipment effectively (Table 5). Other skills like crime prevention, First Aid, emergency procedures, and crisis management registered slightly lower levels of training but were still implemented by more than 90 percent of respondents.

In terms of expectations in managing a crisis situation, at least 80 percent of respondents expected Crisis Management team members to have the skills to manage crises and implement emergency procedures; whilst 91 percent expected First Aid Responders to be able to render First Aid. Seventy-eight percent of respondents expected their generic hotel employees to have skills to prevent crime. 70 percent expected them to implement emergency procedures. A lower percentage (60 percent) expected them to have skills to implement anti-terrorism efforts.

**Table 4: Type of Systems Adopted in Respondent Hotels**

| Type of Systems | Yes (%) | No (%) | Unsure (%) |
|---|---|---|---|
| Access Control Systems - may include locks, signage, barriers, controlled lift access etc. | 98.0 | 0.0 | 2.0 |
| Surveillance Systems - may include CCTV, roving patrols, regular patrols, monitors etc. | 96.0 | 2.0 | 2.0 |
| Security Systems - may include X Ray machines, security command and control etc. | 81.6 | 10.2 | 8.2 |
| Alarm Systems - may include duress alarm, cashier counter alarms, fire alarm etc. | 94.0 | 4.0 | 2.0 |
| Communications Systems - may include PA system, emergency phone, signage, notices, independent phone system etc. | 98.0 | 0.0 | 2.0 |
| Crisis Information Management Systems - may include early warning systems, emergency notification and dispatch systems, social media systems etc. | 91.8 | 0.0 | 8.2 |
| Information Technology Systems - may include property management systems, IT alternate sites, data centre controls, data centre recovery etc. | 91.8 | 2.0 | 6.2 |
| Emergency Systems- may include sprinklers, alarms, detectors etc. | 96.0 | 2.0 | 2.0 |
| Evacuation and Shelter Systems - may include emergency escape routes, save haven rooms etc. | 94.0 | 0.0 | 6.0 |

***Source:*** Survey conducted by author from 28 April to 30 May 2017

**Table 5: Required Skills of Staff**

| Required Skills | Full Time Security Staff (%) | Crisis Manage-ment Team (%) | First Aid Responders (%) | Generic Hotel Employees (%) |
|---|---|---|---|---|
| Standard Operating Procedures | 100.0 | 79.1 | 74.4 | 74.4 |
| Crime Prevention | 97.6 | 65.9 | 43.9 | 78.0 |
| Anti-Terrorism | 100.0 | 75.0 | 55.0 | 60.0 |
| Handling Security Incidents | 100.0 | 59.5 | 26.2 | 26.2 |
| Crowd and Traffic Control | 100.0 | 34.1 | 17.1 | 22.0 |
| Handling Security and Emergency Equipment | 100.0 | 47.6 | 35.7 | 7.1 |
| First Aid Skills | 95.3 | 46.5 | 90.7 | 25.6 |
| Crisis Management | 90.5 | 88.1 | 31.0 | 19.0 |
| Emergency Procedures | 95.3 | 81.4 | 74.4 | 69.8 |

***Source:*** Survey conducted by author from 28 April to 30 May 2017

Respondents were also asked to indicate the type of training programmes that staff was sent for (Table 6) and resources provided for their staff to perform their duties. A review of the Tables 5 and 6 indicate that respondents provided the necessary training for their security and crisis management staff to acquire the required skills – including managing terrorist threats.

**Table 6: Training Programmes for Staff**

| Training Programmes | Full Time Security Staff (%) | Crisis Manage-ment Team (%) | First Aid Responders (%) | Generic Hotel Employees (%) |
|---|---|---|---|---|
| Standard Operating Procedures | 97.6 | 82.9 | 78.0 | 73.2 |
| Crime Prevention | 100.0 | 61.0 | 39.0 | 61.0 |
| Anti-Terrorism | 100.0 | 74.4 | 46.2 | 51.3 |
| Handling Security Incidents | 100.0 | 52.5 | 22.5 | 17.5 |
| Crowd and Traffic Control | 100.0 | 35.0 | 10.0 | 17.5 |
| Handling Security and Emergency Equipment | 100.0 | 51.2 | 31.7 | 7.3 |
| First Aid Skills | 93.0 | 46.5 | 90.7 | 27.9 |
| Crisis Management | 90.2 | 90.2 | 31.7 | 26.8 |
| Emergency Procedures | 95.2 | 85.7 | 76.2 | 71.4 |

***Source:*** Survey conducted by author from 28 April to 30 May 2017

Respondents also indicated the types of training formats used (Table 7). The most common format utilised was the circulation of guidelines and procedures, followed by classroom sessions where procedures were discussed and presented to employees. Table-Top exercises and drills were also found to be widely utilised for training in crisis management and emergency procedures. Computerised Simulation Games were rarely utilised for training purposes of any kind.

All respondents were satisfied or very satisfied with the training programmes that their security staff was sent for. This satisfaction was evidenced by 86 percent of their crisis management team, 95 percent of their First Aid responders, and 87.5 percent of their generic hotel employees. The respondents were also asked to rank the training formats that were suitable to train staff for terrorist attacks (Table 8). With respect to the most suitable format, 54 percent selected Drills and Exercises, 17 percent respondents chose Guidelines and Procedures, and the remaining three choices i.e. Classroom Sessions, Table-Top Exercises, and Simulation Games each attracted 10 percent of the responses. At the other end of the scale, 34 percent of respondents ranked Computer simulation games as the least appropriate for such training purposes.

**Table 7: Training Formats Used by Hotels**

| Training Formats | Guidelines and Procedures (hard and/or soft copy) (%) | Classroom Sessions (talks, seminars etc.) (%) | Table-Top Exercises (%) | Drills and Exercises (%) | Simulation Games (computer based) (%) |
|---|---|---|---|---|---|
| Standard Operating Procedures | 100.0 | 71.4 | 59.5 | 64.3 | 7.1 |
| Crime Prevention | 92.3 | 76.9 | 48.7 | 46.2 | 5.1 |
| Anti-Terrorism | 92.1 | 78.9 | 65.8 | 55.3 | 7.9 |
| Handling Security Incidents | 100.0 | 67.5 | 47.5 | 45.0 | 2.5 |
| Crowd and Traffic Control | 94.6 | 43.2 | 35.1 | 32.4 | 2.7 |
| Handling Security and Emergency Equipment | 94.9 | 64.1 | 38.5 | 56.4 | 2.6 |
| First Aid Skills | 84.6 | 89.7 | 38.5 | 61.5 | 5.1 |
| Crisis Management | 95.0 | 77.5 | 82.5 | 55.0 | 7.5 |
| Emergency Procedures | 97.6 | 78.0 | 82.9 | 80.5 | 4.9 |

***Source:*** Survey conducted by author from 28 April to 30 May 2017

**Table 8: Most Effective Training Format for Anti-Terrorism Skills**

| | Most Effective | | | | Least Effective |
|---|---|---|---|---|---|
| **Training Formats** | **1 (%)** | **2 (%)** | **3 (%)** | **4 (%)** | **5 (%)** |
| Guidelines and Procedures (hard and/or soft copy) | 17.1 | 24.4 | 17.1 | 19.5 | 22.0 |
| Classroom Sessions (talks, seminars etc) | 9.8 | 14.6 | 29.3 | 26.8 | 19.5 |
| Table Top Exercises | 9.8 | 31.7 | 22.0 | 29.3 | 7.3 |
| Drills and Exercises | 53.7 | 9.8 | 12.2 | 7.3 | 17.1 |
| Simulation Games (computer based) | 9.8 | 19.5 | 19.5 | 17.1 | 34.1 |

***Source:*** Survey conducted by author from 28 April to 30 May 2017

Respondents were then asked to view the video clip of a computer simulation game[10] designed for Shopping Mall security staff and surveyed on their awareness of Computer simulation games as a training option. Forty percent respondents indicated

[10] TribeStudios08. Security Training and Simulation System (STSS). March 15, 2016. https://www.youtube.com/watch?v=A9ppeQTWP8w (accessed June 05, 2017).

that they were unaware, and only 10 percent had used these games for training purposes. Eighty-five percent of respondents expressed interest in sending their staff for Computer Simulation Game training, if it was made available to them.

## DISCUSSION AND CONCLUSION

Singapore hotels are taking the terrorism threat seriously. All respondents confirmed that their security staff needed to have anti-terrorism skills. While this is an obvious consideration for security personnel, 75 percent of respondents expected the same from their crisis management team and 60 percent expected their general hotel employees to be similarly equipped (Table 5). The respondents demonstrated their seriousness by ensuring that staff was trained to have these skills; i.e. all respondents provided anti-terrorism training for their security staff. However, only 51 percent of generic hotel employees (who make up the majority of hotel employees) received such training (Table 6). This is of concern as the generic hotel employee would likely be among the first-line employees to encounter the perpetrators of a terrorist attack and should be able to respond effectively.

In view of the increasingly important role that private sector's security professional play in the fight against terrorism (Khair, 2017), it is important that a set of common standards in terms of training and operations be widely adopted in the industry. The findings indicated that 60 percent of respondents had security policies based on the ISO standard[11]. BCM policies fared worse at only 44 percent. This variability on policies between individual hotels can affect the effectiveness of collaborative efforts between the public and private sector in the event of a crisis. The government is cognizant of this and has introduced training programmes incorporating these standards under *Project Guardian* and other schemes.

Drills and exercises are the best training formats to accomplish this and the government agencies and hotels have been conducting joint exercises for this reason. However, each exercise can involve a limited number of hotel participants at any one point in time. Furthermore, the frequency and duration of such training will be limited due to the high cost and disruptive nature of such exercises in everyday hotel functioning.

Computer simulation games can therefore serve as an intermediate format where staff can learn and practice responses that conform to government standards. Security and Crisis Management staff can experience scenarios re-enacting actual attacks in other countries that provide a level of realism whilst keeping disruptions to normal business operations to a manageable level. These scenarios can be updated based on available counter-terrorism intelligence from the authorities.

[11] The proportion of large hotels (those with more than 300 rooms) fared worse with only 53 percent reported having security plans based on the ISO Standard.

The type of training can be programmed on a modular basis. All staff could be provided with basic anti-terrorism training; e.g. handling of suspicious packages/articles. In addition, staff from the housekeeping, front desk, food and beverage, and maintenance departments could sit for customised modules that simulate scenarios from their unique perspectives. For example, housekeeping staff could practice their responses (when cleaning hotel rooms used by terrorists) by recognising tell-tale signs of attack planning; such as the presence of confidential material, hotel blueprints, and staff schedules (Department of Homeland Security, 2010). Front desk staff could be trained to spot suspicious unattended vehicles, and security staff could be trained to manage security cordons. A key advantage is that the staff can be assessed immediately after completing the training. These records can be made available via online "cloud" to the hotel, and maintained in hotel computer archives.

Computer simulation games are also scale-able, i.e. the games could be designed on mobile smartphone platforms that could train large numbers of staff on their own mobile devices at their own convenience (Chittaro, 2016). However, trainees will only take their training seriously if the simulations are well-designed. Studies have shown that participants responded emotionally to games that were realistic (Wyke, 2015) and interactive (Chittaro and Sioni, 2015).

In conclusion, hotels should continue with their existing modes of training, i.e. guidelines, classroom sessions, and drills; but supplement them with Computer simulation games as part of a complete suite of training tools for their staff to use.

## LIMITATIONS

The Singapore Hotel Association circulated the survey link via email addressed to the General Managers of member hotels. These were forwarded to the relevant security and operations managers who then responded to the survey. Whilst the target respondents answered the survey, it is difficult to verify that their responses reflected the true nature of the hotel's situation or were tailored to promote a public impression that the hotel management desired to promote. The issue of false-positive bias, i.e. managers granting positive scores for their own programmes is not eliminated in this survey.

As the survey was an online survey, it is difficult to verify that the respondents viewed the video case studies as requested. These videos served an important role as they provide the context for latter questions.

The respondents were full-time staff, wholly involved in the day-to-day operations of the hotels they were employed at. The respondents were informed that it would take about 15 minutes to complete the survey. Using the time between the survey's initiation and completion date-time stamp, the respondents took longer than the estimated time to complete the survey – some even lasting for a few days. Whilst the respondents could complete the survey in stages, i.e. more than one sitting over

the course of a few days; it is difficult to verify that the surveys were completed by the same respondent throughout.

These concerns can be verified in follow-up interviews with the respondents and their General Managers separately, and sighting of training records and other documentation. In view of the time constraint, this was not completed but will be implemented in future studies.

## RECOMMENDATIONS FOR FUTURE WORK

This study is a first step to review the BCM practices of Singapore Hotels from the perspective of hotel security and operations staff. It attempts to cover as wide a base as possible. Future studies that probe deeper into the BCM practices of selected hotels could provide a better cross-sectional perspective of their security and training programmes to manage terrorist threats.

Studies could be conducted to explore the effectiveness of government agencies, and to explore the effectiveness of increased public-private training collaborations. However, such findings would likely remain confidential due to their sensitive nature.

Lastly, Nanyang Polytechnic (NYP) will explore the development of a Computer Simulation Game Platform to train employees from interested hotels. Collaborative efforts with relevant government authorities could be explored to incorporate the minimum standards expected from the private sector, covering areas within the training scope of the *Project Guardian* Scheme. A comparative study on the effectiveness of the hotels' training programmes, before and after their participation in this Computer Simulation Game, will be useful to assess the validity of the observations made in this study. NYP can also explore virtual reality platforms to provide a more immersive experience for trainees from the hotel industry in the near future.

## REFERENCES

Barta, Patrick; Carder, Reuben. "Police Say Bombers Sought Higher Toll". *Wall Street Journal*, (27 July 2009).

Building and Construction Authority, Singapore Civil Defence Force, Internal Security Department and Singapore Police Force, *Enhancing Building Security – Useful and Practical Measures*, Singapore 2005

Chittaro, Luca, and Riccardo Sioni. "Serious games for emergency preparedness: Evaluation of an interactive vs. a non-interactive simulation of a terror attack." *Computers in Human Behavior* 50 (2015): 508-519.

Chittaro, Luca. "Designing Serious Games for Safety Education: "Learn to Brace" versus Traditional Pictorials for Aircraft Passengers." *IEEE transactions on visualization and computer graphics* 22, no. 5 (2016): 1527-1539.

Department of Homeland Security. *"No Reservations - Suspicious Behavior in Hotel."* FLV, 9:17, (2010). https://www.dhs.gov/video/no-reservations-suspicious-behavior-hotels (accessed July 20, 2017)

Engemann, Kurt J., and Douglas M. Henderson. *Business Continuity and Risk Management: Essentials of Organizational Resilience.* Rothstein Publishing, 2011.

Gunaratna, Rohan. "The post-Madrid face of Al Qaeda." *The Washington Quarterly* 27, no. 3 (2004): 91-100.

Harwood, M. "Hotels become a favorite target for terrorists" ASIS International, 10 September 2009, https://sm.asisonline.org/migration/Pages/hotels-become-a-favorite-target-terrorists-006186.aspx (accessed August 4, 2017).

Ho, P K. Speech at the Hotel Security Conference cum Hotel Security Award Presentation, 4 Nov 1996; http://www.nas.gov.sg/archivesonline/speeches/record-details/77ea9f17-115d-11e3-83d5-0050568939ad (accessed July 20, 2017)

Homefront Security Division, *Guidelines for Enhancing Building Security in Singapore (GEBSS),* Singapore, Ministry of Home Affairs, 2010.

Jayakumar, S., Senior Minister/Coordinating Minister for National Security. Opening Speech at the 2009 National Security Dialogue with the Business Community, 4 Aug 2009; https://www.mfa.gov.sg/content/mfa/media_centre/press_room/sp/2007/200705/speech_20070529.html (accessed July 20, 2017)

Khair, Muhamad." Orchard Road Counter-Terrorism Seminar: How Ready Are We?" *Home News*, July 19, 2017. https://www.hometeam.sg/article.aspx?news_sid=20170719x5DTbZsg 06hR (accessed July 20, 2017).

Lee, H L. Speech at Official Launch of SGSecure, 24 Sep 2016 http://www.pmo.gov.sg/newsroom/pm-lee-hsien-loong-official-launch-sgsecure (accessed July 20, 2017)

McMullan, Caroline, and Tom Baum. "Crisis management: Towards a model of good practice for small to medium sized hotels." In *Proceedings of the 1st International Conference in Safety and Crisis Management in the Construction, Tourism and SME Sectors*, p. 100. Universal-Publishers, 2011.

Ministry of Home Affairs, The Jemaah Islamiyah arrests and the threat of terrorism : white paper. (Ministry of Home Affairs Singapore 2003). https://www.mha.gov.sg/Newsroom/speeches/Documents/English.pdf (accessed June 6, 2017)

Ministry of Home Affairs. "Singapore Terrorism Threat Assessment Report 2017." Press release, June 1, 2017. https://www.mha.gov.sg/newsroom/press-releases/Pages/Singapore-Terrorism-Threat-Assessment-Report-2017.aspx (accessed July 20, 2017)

Onishi, N. "Indonesia Bombings Signal Militants' Resilience." *New York Times*, July 17, 2009. http://www.nytimes.com (accessed Aug 4, 2017)

Shanmugam, K. Speech at Milipol Asia Pacific 2017, 5 Apr 2017. https://www.mha.gov.sg/newsroom/speeches/Pages/The-Inaugural-Milipol-Asia-Pacific-2017-Marina-Bay-Sands.aspx (accessed July 20, 2017)

Singapore Police Force. “Prevent Terrorism”. (last modified April 21, 2016) https://www.police.gov.sg/resources/prevent-terrorism/project-guardian

Singapore Standards for Hotel Security SS 545:2009, 2015

Singapore Standards Societal Security, Business Continuity Management systems, Guidance SS ISO 22313:2013

Smith, David. "Business continuity and crisis management." *Management Quarterly* 44, no. 1 (2003): 27-33.

Stewart, Scott. “Employees, the First Line of Defense Against Jihadist Insiders.” *Stratfor* Aug 11, 2016. https://worldview.stratfor.com/weekly/employees-first-line-defense-against-jihadist-insiders (accessed September 3, 2016)

*Straits Times*, “Body parts: Anatomy of a killing” November 12 1995.

*Straits Times*, “Indonesian suspect arrested over plot to attack Marina Bay was planning to work in Sentosa as a cleaner”. September 5, 2016. http://www.straitstimes.com (accessed June 6, 2017).

*Straits Times*, “Two men sought for attack on two Japanese tourists.” June 8 1994.

Strohschneider, Stefan, and Jürgen Gerdes. "MS ANTWERPEN: Emergency management training for low-risk environments." *Simulation & Gaming* 35, no. 3 (2004): 394-413.

Susi, Tarja, Mikael Johannesson, and Per Backlund. "Serious games: An overview." Skövde: University of Skövde (Technical Report HS-IKI-TR-07-001), 5 February 2007.

Tellis, Ashley J., Robert D. Blackwill, Peter Chalk, Kim Cragin, C. Christine Fair, Brian A. Jackson, Brian Michael Jenkins, Seth G. Jones, Nathaniel Shestak, and Angel Rabasa. "The lessons of Mumbai." *Santa Monica, Calif.: RAND* (2009).

*Today*, “Attack on Singapore a matter of when, not if, says Shanmugam”. March 23, 2016. http://www.todayonline.com (accessed on October 4, 2016).

Wyke, T. "Virtual Reality simulator where players live out the horrific final moments of 9/11 terror attack victims is condemned as 'sick'." *Mail Online*, October 30, 2015. (accessed May 02, 2016). http://www.dailymail.co.uk/news/article-3296767/Virtual-Reality-simulator-players-live-horrific-final-moments-9-11-terror-attack-victims-condemned-sick.html. (accessed July 2, 2017)