



Global
Alliance



Innovate
UK

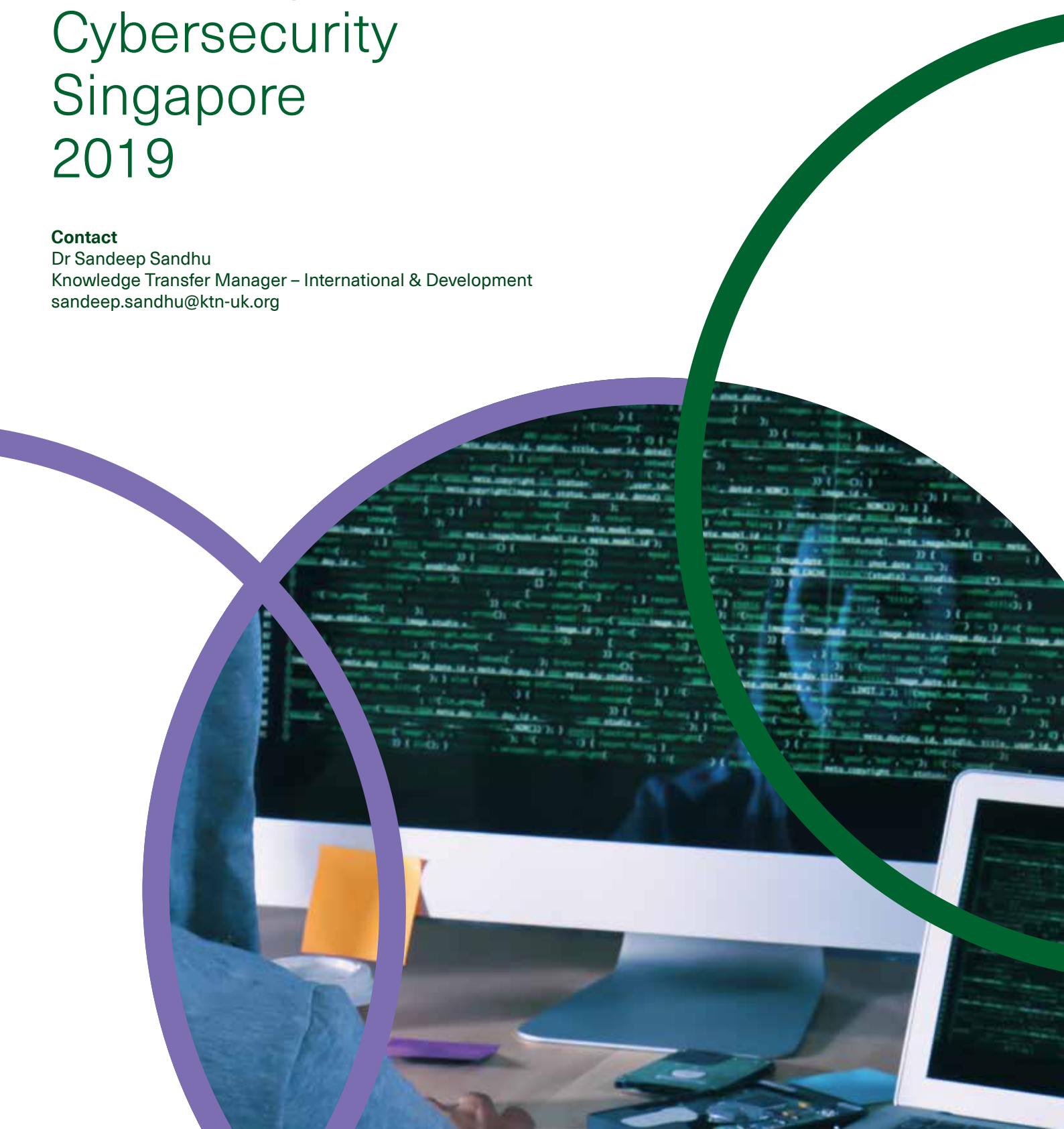
Connecting for
Positive Change

—
ktn-uk.org/Global

Global Expert Mission Cybersecurity Singapore 2019

Contact

Dr Sandeep Sandhu
Knowledge Transfer Manager – International & Development
sandeep.sandhu@ktn-uk.org





Contents

Welcome	4
1 Introduction	5
2 The Singapore Market	6
2.1 Economic Snapshot	6
2.2 The Cybersecurity Market	7
2.2.1 Market Opportunities	7
2.3 Singapore and Start-ups	8
3. The Singapore Cybersecurity Ecosystem	11
3.1 Government	11
3.1.1 The Cybersecurity Agency (CSA)	11
3.1.2 The National Research Foundation (NRF)	11
3.1.3 Ministry of Home Affairs	12
3.1.4 The Economic Development Board (EDB)	12
3.1.5 Enterprise Singapore	13
3.1.6 Skills	13
3.2 Academia	13
3.2.1 National University Of Singapore (NUS)	13
3.2.2 Nanyang Technological University (NTU)	14
3.2.3 A*Star	14
3.2.4 I-Trust – Centre For Research in Cybersecurity	15
3.3 Industry	15
3.3.1 Ensign Infosecurity	15
3.4 Collaborative Efforts	16
3.4.1 Singapore Cybersecurity Consortium	16
4. Coming To Singapore	17
4.1 Start-up and Investor Landscape	17
4.2 Ice71	17
4.3 Enterprise Singapore	18
4.4 Singtel Innov8	18
4.5 Temasek	19
4.5.1 The Global Cybersecurity Platform	19
5 Collaboration	20
5.1 Existing UK-Singapore Collaboration	20
5.2 Challenges	21
Annex 1 – List of UK and Singapore Participants	22

Welcome

Innovate UK's global missions programme is one of its most important tools to support the UK's Industrial Strategy's ambition for the UK to be the international partner of choice for science and innovation. Global collaborations are crucial in meeting the Industrial Strategy's Grand Challenges and will be further supported by the launch of a new International Research and Innovation Strategy.

Innovate UK's Global Expert Missions, led by Innovate UK's Knowledge Transfer Network, play an important role in building strategic partnerships, providing deep insight into the opportunities for UK innovation and shaping future programmes.

In October 2019, the Singapore Cybersecurity Expert Mission travelled to Singapore to meet with stakeholders in the public and private sector including government agencies, academia, industry and investors to better understand the cybersecurity landscape and identify opportunities for collaboration.

In this publication we share the information and insights gathered during the delegation's time in Singapore.

1. Introduction

Singapore has been experiencing an exponential growth in technology start-ups combined with innovation and digital transformation in its core industries. This phenomenon has led to cybersecurity becoming a national priority. The city-state has identified four pillars to innovation: digital economy, sustainable technology, defence and security, and education.

The Expert Mission to Singapore in October 2019 aimed to better understand the cybersecurity landscape, the roles played by the various stakeholders within the local ecosystem (public and private), the key priorities and most importantly the opportunities and mechanisms for collaboration between Singapore and the UK. The mission involved meetings with representatives of the Singapore government and its agencies including:

- the Cybersecurity Agency (CSA)
- the National Research Fund (NRF)
- the Economic Development Board (EDB)
- the Ministry of Home Affairs.

Academia was represented by the National University of Singapore (NUS) and Nanyang Technological University (NTU) with a focus on their specific activity in cybersecurity. The Singapore Cybersecurity Consortium represented the collaboration between government, academia and industry. Private sector engagement during the mission involved meeting with the key cybersecurity accelerators in Singapore, the largest home-grown cybersecurity company, several cybersecurity start-ups that have chosen Singapore as their primary location and established multinationals which are using Singapore as a platform for countries in the Association of Southeast Asian Nations (ASEAN) region.

Singapore views the UK as a natural partner given historical ties and similar legal systems, and there is wide recognition of both the need and opportunity to collaborate. As Singapore marks the bicentennial of Sir Stamford Raffles' arrival and the UK begins a new era, both countries have reignited their partnership to broaden and deepen ties in the years ahead.¹ The partnership is aimed at building on existing links and strengthening collaboration.

Southeast Asia's growing political, economic and strategic significance means that it is critical that the UK forges strong ties with the region. This relationship will be vital for the UK's influence, prosperity and national security and will in turn also benefit Singapore. It is imperative that the UK is well-positioned to take advantage of the continuing prosperity in the region and helping to ensure that this is underpinned by regional stability and security.² Within this context, closer collaboration on innovation and research and development (R&D) with partners in Singapore between government agencies, between academics and industry, will form a crucial component of the UK's approach.

¹ <https://www.straitstimes.com/singapore/spore-uk-launch-partnership-to-forge-broader-deeper-ties>.

² <https://www.gov.uk/guidance/building-prosperity-and-supporting-security-in-south-east-asia>.

2. The Singapore Market

2.1 Economic Snapshot

Singapore has a population of only 5.5 million people (smaller than Israel) and half the size of Greater London. The economic stability of the region acts as a barometer for the world, with a large amount of international trade passing through the country. A lack of trade for the ASEAN region equates to a lack of trade for Singapore.

Approximately 20% of Singapore’s GDP is derived from the manufacturing sector, with the lion’s share sourced from services. There is a pro-business attitude throughout the region. There has been considerable investment in infrastructure, partly due to one of the most modern ports in the world. Singapore acts as a regional gateway with strong connectivity, and it aspires to play a regional leadership role in cybersecurity.

There is approximately US\$13 billion trade between the UK and Singapore a year and approximately US\$40 billion of bilateral investment.³

Singapore is part of the ASEAN economic community to encourage integration and freer trade flow. Although there are big aspirations for ASEAN integration, this is slow-paced.

The British High Commission in Singapore has observed the following:

- Indonesia – A trillion-dollar market with stable growth focused on reform.

- Thailand – Underperforming but has strong potential.
- Malaysia – Good positive growth.
- Singapore – Economic restructuring via “future economy and smart nation” aspirations.
- Philippines – Top performers, despite the recent disruption caused by the war on drugs.
- Vietnam – New cyber law, shows a high focus on cyber. However, the law is focused on government-citizen introspection rather than protecting the people or their business/assets.

In essence, the ASEAN region’s potential is characterised by:

- its growing economic weight;
- ten diverse economies;
- regional connectivity (trade agreements and global supply chains);
- the ASEAN economic community; and
- a vast opportunity in the consumer-focused sectors.

2.2 The Cybersecurity Market

Singapore has made rapid progress in developing its global position as a leader in cybersecurity. Whilst its entry on the global stage is recent and is still immature in comparison to its core competitors: the US, Israel and the UK, it is fast becoming a leading hub for cybersecurity – particularly in the Southeast Asian region but with global ambitions and potential. The

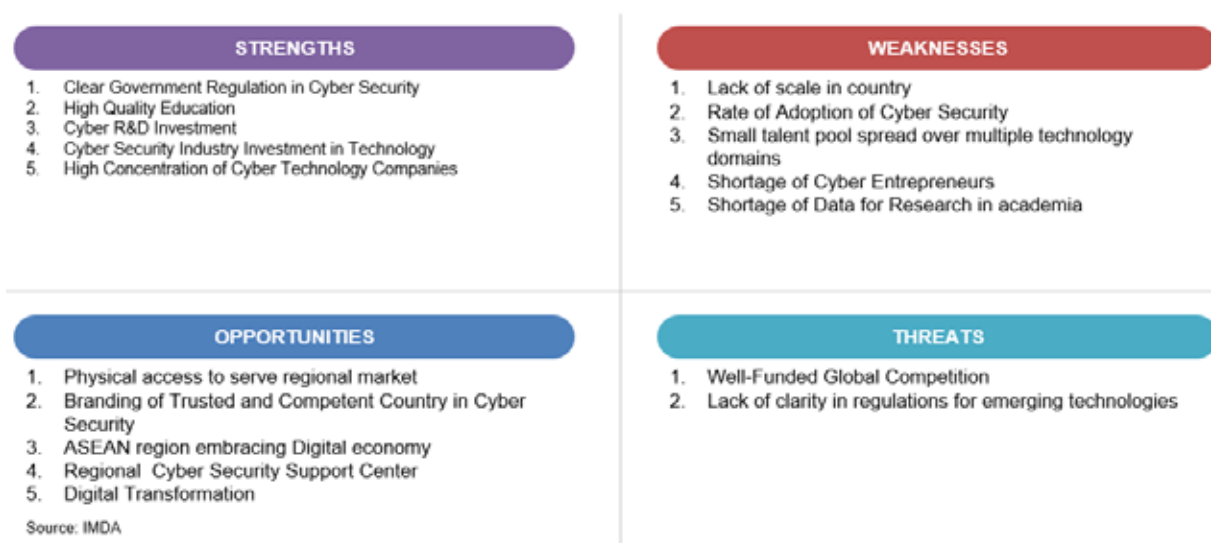


Figure 1 Singapore Cybersecurity Market SWOT Analysis

Source: Info-Communications Department, Singapore Government, Future of Services Report, Annex A-3

³ <https://oec.world/en/profile/country/sgp/>

UN Global Cybersecurity Index ranked Singapore as the top nation in the world for its commitment to cybersecurity. The cybersecurity market in Singapore was worth approximately US\$500 million in 2017 and is expected to grow, reaching approximately US\$900 million by 2022, with a 15% Compound Annual Growth Rate (CAGR).⁴

The Singapore market reveals strengths, weaknesses, opportunities and threats as indicated in Figure 1. Development of the cybersecurity market and future growth will need to take into account these factors and will require clear, focused strategic leadership.

Singapore already has active R&D efforts demonstrated by investments from industry and local research institutes, aiming to meet increasing demands from global and local cybersecurity players.

Examples of this R&D effort were witnessed during the mission. Both NTU and NUS have ongoing collaborations and investment from the Singapore government, Singtel and others.

The delegation also observed that Singapore has a rather technical approach when it comes to cybersecurity, both in industry and in government.

2.2.1 Market Opportunities

UK companies providing solutions or services in the areas listed in the table below should find opportunities in Singapore and the wider ASEAN region.⁵ Opportunities to collaborate on the development of those products and services for the local markets or to partner with existing local organisations to gain access to these new markets clearly exist.

PRODUCTS/SOLUTIONS

Identity and access management

Advanced endpoint, network and cloud security

Threat and vulnerability management

ICS (industrial control systems) and Scada (supervisory control and data acquisition) security

Critical infrastructure information

Artificial intelligence

Data analytics and protection

Internet of Things (sensor technology)

Blockchain and distributed ledger technology

⁴ <https://www2.imda.gov.sg/-/media/Imda/Files/Industry-Development/Infrastructure/Technology/Technology-Roadmap/WG3-Cyber-Security-Executive-Summary.pdf>

⁵ Cybersecurity Opportunities in the ASEAN Region 2018. Australia Trade and Investment Commission and the Australian Cybersecurity Growth Network.

2.3 Singapore and Start-ups

The delegation learned that, within Singaporean families, becoming a tech entrepreneur or working in a start-up is not seen as a legitimate route to success by many, in comparison to a more conventional career in finance or joining an established global technology company. However, this risk-averse attitude is starting to change, and Singapore is doing considerably well for its size. (This graph shows that Singapore has slipped two places in the rankings since 2017.)

“Singapore and Silicon Valley share a unique quality; they are magnets for talent across the globe. Magic is sparked when people from different backgrounds come together to solve a problem.”

Vinnie Lauria,
Managing Partner at Golden Gate Ventures

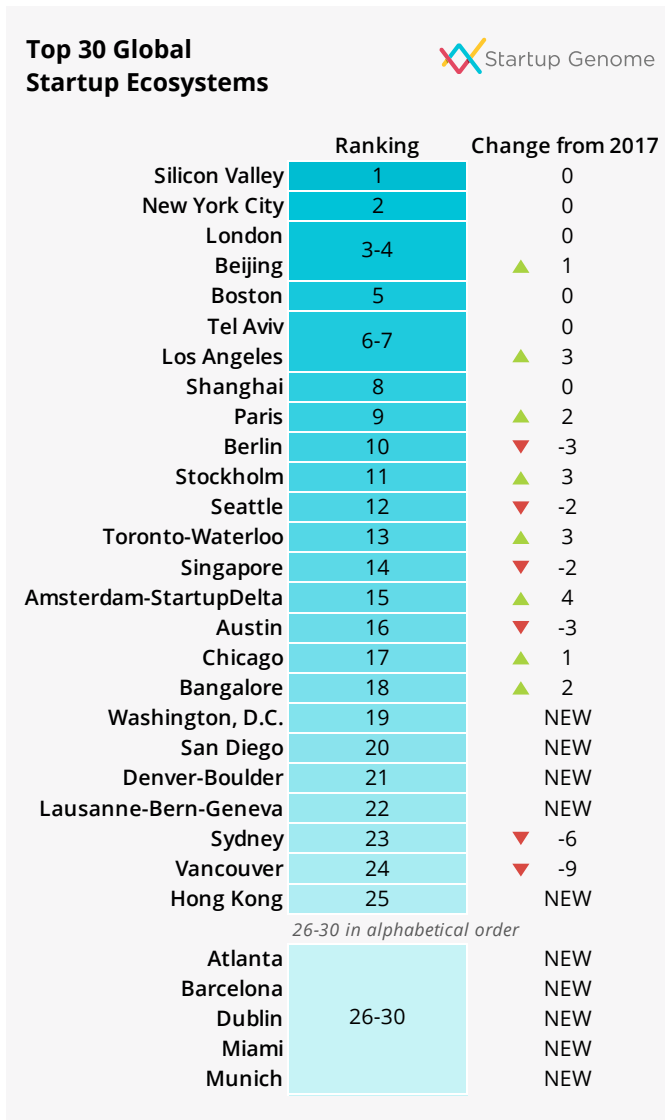



Figure 2 The Top 30 Global Start-up Ecosystems
Source: Start-up Genome, Global Start-up Ecosystem Report 2019

Indeed, Singapore’s position amongst the top 30 global ecosystems for start-ups in the world is impressive given its size and cultural tendencies towards risk aversion.

2019 Global Startup Ecosystem Ranking



Ranking	Change from 2017	Performance	Funding	Market Reach	Connectedness	Talent	Experience	Knowledge	Growth Index
Silicon Valley	1	0	1st	1st	1st	1st	1st	1st	5
New York City	2	0	1st	1st	3rd	2nd	2nd	1st	6
London	3-4	0	1st	1st	1st	1st	2nd	2nd	6
Beijing	▲ 1	1st	1st	5th	5th	1st	1st	1st	4
Boston	5	0	1st	2nd	2nd	3rd	1st	1st	7
Tel Aviv	6-7	0	2nd	2nd	2nd	1st	2nd	1st	6
Los Angeles	▲ 3	1st	1st	3rd	4th	3rd	2nd	3rd	5
Shanghai	8	0	2nd	2nd	2nd	4th	1st	3rd	6
Paris	▲ 2	2nd	1st	3rd	2nd	3rd	3rd	2nd	8
Berlin	▼ -3	3rd	2nd	1st	1st	2nd	3rd	4th	6
Stockholm	▲ 3	3rd	2nd	2nd	2nd	4th	2nd	2nd	7
Seattle	▼ -2	2nd	3rd	3rd	3rd	1st	1st	3rd	5
Toronto-Waterloo	▲ 3	3rd	2nd	1st	3rd	4th	4th	3rd	5
Singapore	▼ -2	2nd	4th	4th	1st	2nd	3rd	4th	5
Amsterdam-StartupDelta	▲ 4	2nd	3rd	5th	3rd	5th	4th	3rd	7
Austin	▼ -3	3rd	3rd	4th	4th	1st	1st	3rd	5
Chicago	▲ 1	3rd	4th	4th	5th	3rd	4th	5th	4
Bangalore	▲ 2	3rd	4th	5th	2nd	4th	4th	2nd	7
Washington, D.C.	NEW	4th	3rd	3rd	5th	4th	2nd	4th	5
San Diego	NEW	4th	3rd	4th	4th	3rd	3rd	4th	6
Denver-Boulder	NEW	4th	4th	4th	4th	3rd	2nd	4th	7
Lausanne-Bern-Geneva	NEW	4th	4th	2nd	3rd	5th	5th	2nd	9
Sydney	▼ -6	5th	5th	5th	2nd	4th	5th	5th	7
Vancouver	▼ -9	4th	5th	1st	3rd	3rd	3rd	3rd	6
Hong Kong	NEW	5th	5th	2nd	1st	4th	5th	5th	6
<i>26-30 in alphabetical order</i>									
Atlanta	NEW	5th	5th	4th	5th	2nd	4th	5th	4
Barcelona	NEW	5th	4th	5th	4th	5th	5th	5th	6
Dublin	NEW	5th	3rd	5th	5th	5th	4th	5th	5
Miami	NEW	4th	5th	1st	5th	5th	5th	4th	5
Munich	NEW	5th	5th	3rd	2nd	5th	5th	1st	7

Top ranked ecosystems classified in tiers from 1st (top) to 5th

Figure 3 Global Start-up Ecosystem Ranking
 Source: Start-up Genome, Global Start-up Ecosystem Report 2019

The table above indicates that Singapore ranks amongst the best for connectedness and talent. London ranks third after Silicon Valley and New York.

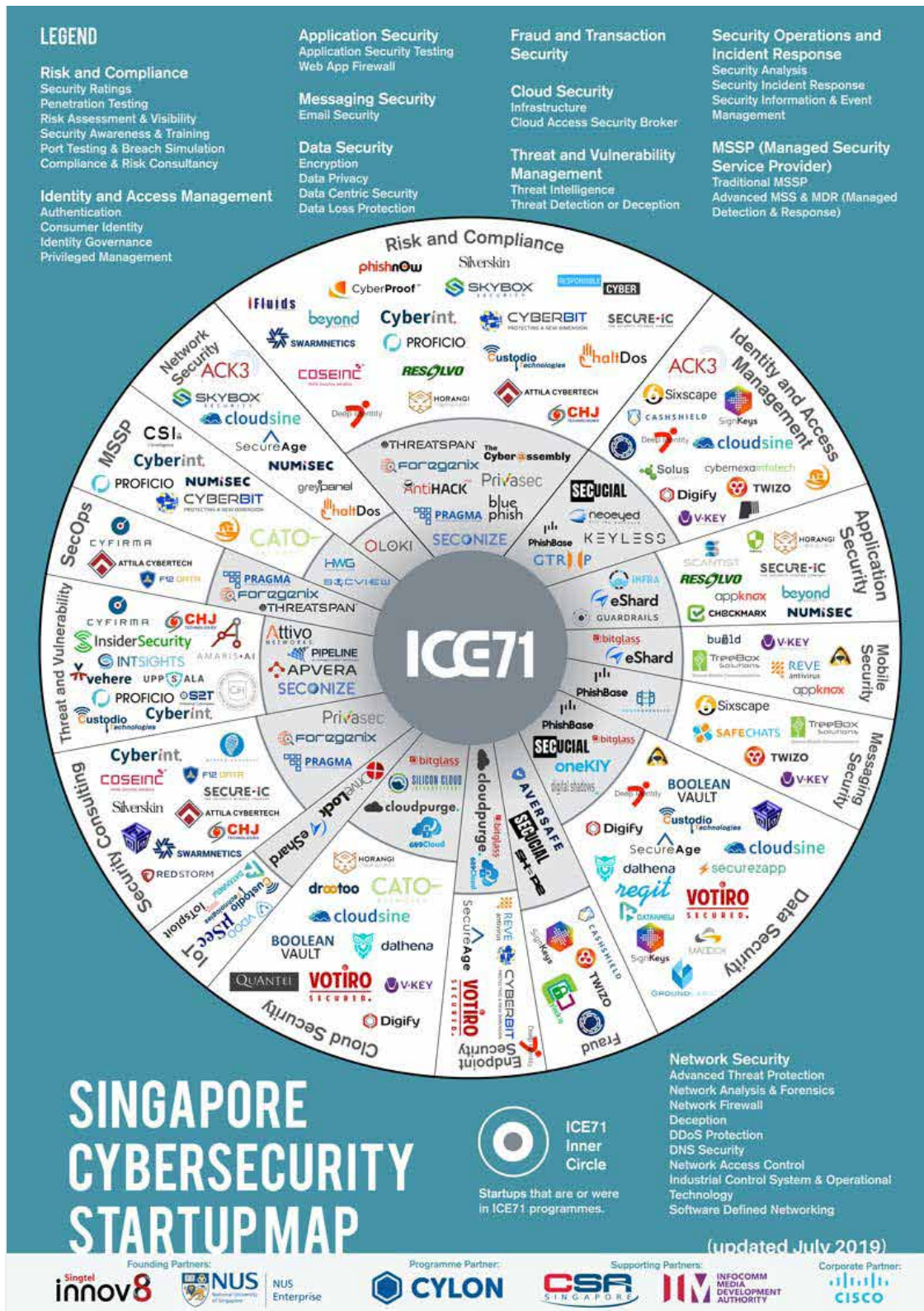


Figure 4 Singapore Cybersecurity Start-up Map

The map above shows a vibrant start-up scene within the realm of cybersecurity with considerable diversity covering a number of aspects within the overall threat landscape.

The ease of doing business in and from Singapore, coupled with attractive tax incentives, also make it an appealing destination for foreigners to set up and start their business.

3. The Singapore Cybersecurity Ecosystem

In 2013, Singapore launched the five-year National Cybersecurity Masterplan 2018⁶ which was aimed at securing Singapore's cyber environment. This Masterplan was a multi-agency effort coordinated by the Info Communications Media Development Authority of Singapore (IMDA)⁷ under the guidance of the National Infocomm Security Committee.

One of the outcomes of this was the creation of CSA in 2015 to develop a national strategy for cybersecurity. This strategy was launched in 2016 with the intention of coordinating the public and private sector efforts to protect critical information infrastructure (CII) including power, transport, telecoms, airports and financial services. The strategy sets out Singapore's vision, goals and priorities for cybersecurity. Alongside coordination within Singapore, the strategy emphasises the need for international partnerships to ensure trust and resilience in cyberspace.

3.1 Government

The delegation met with several government stakeholders including the CSA, NRF, Ministry of Home Affairs, the EDB and Enterprise Singapore. This section outlines the discussions during those meetings.

3.1.1 The Cybersecurity Agency (CSA)

The Cybersecurity Agency (CSA)⁸ is a national agency overseeing cybersecurity strategy, operation, education, outreach, and ecosystem development. It is part of the Prime Minister's Office and is managed by the Ministry of Communications and Information.

The CSA is developing a robust cybersecurity ecosystem and a vibrant, dynamic industry, well-resourced with the talent and capacity to respond to and mitigate cyber-attacks. The ecosystem needs to be a sustainable source of expenditure and solutions, bringing about economic opportunity and jobs.

The CSA has a commitment to advance capabilities through R&D. This is achieved through a funding programme they run called the CSA Co-Innovation and Development Proof of Concept Funding Scheme.⁹ The scheme aims to support the development of solutions with collaboration between

solution providers and end-users. The scheme is intended to catalyse a critical mass of effort focused on the development of innovative cybersecurity solutions with the demonstrated potential to meet national cybersecurity and strategic needs. This scheme is open to organisations from overseas; however, they must partner with a legal entity in Singapore.

At the same time, the CSA also supports the National Cybersecurity R&D (NCR) Program.¹⁰ This is intended to bring together government agencies, academia, research institutes and industry to collaborate on cybersecurity research. This programme is administered and managed by the NRF.

In essence, the activities of the CSA are all intended to bring about and promote a safer cyberspace where business and society can operate in a trusted and safe cyberspace. The CSA sees collaboration as critical to their overall mission and as such, is keen to see collaboration between the UK and Singapore on challenges that are common to both countries.

3.1.2 The National Research Foundation (NRF)

The National Research Foundation (NRF)¹¹ was created in 2016 as a department within the Prime Minister's Office. It is tasked with setting the direction for R&D through the development of policies and strategy for research and innovation. It funds strategic initiatives and is focused on strengthening R&D capability.

The NRF's main aim is to have a transformational impact on Singapore. This is being enabled by the creation of a vibrant and dynamic R&D hub as part of the push towards a knowledge-intensive, innovative and entrepreneurial economy. The hope is that this will make Singapore more attractive for those seeking excellence in science and innovation. The NRF is looking at cybersecurity from an R&D perspective,

⁶ <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/singapores-national-cybersecurity-masterplan-2018>

⁷ <https://www.imda.gov.sg/>

⁸ <https://www.csa.gov.sg>

⁹ https://www.csa.gov.sg/-/media/csa/documents/poc_scheme/co-innovationproof-of-conceptfundingscheme-infokit3a.pdf

¹⁰ <https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme>.

¹¹ <https://www.nrf.gov.sg/about-nrf/national-research-foundation-singapore>

and a government demand perspective. The CSA drives this primarily, setting the ambition.

The National Cybersecurity R&D Programme (NCR) aims to develop R&D expertise and capability within Singapore. The aim of the programme is to improve trust in critical information infrastructure with an emphasis on security, reliability, resiliency and usability.¹² The programme is coordinated by multiple government agencies within Singapore.

This collaborative coordination is aimed at promoting a joint effort between government agencies, academia, research institutes and the private sector. There are also funding streams in place to encourage small businesses and individuals to solve business problems. This funding is available to anyone who has a registered company in Singapore.

The NRF has allocated SING\$100 million for the cyber R&D plan in 2015. There is approximately a SING\$30 million additional contribution from industry.

Collaboration on funded programmes between the UK and Singapore on R&D has previously taken place through a joint funding programme between the NRF and the Engineering and Physical Science Research Council (EPSRC) in 2015. The areas of focus for this funding are indicated below.

R&D AREAS OF FOCUS
Mobile systems security and cloud
Trustworthy software systems
Design science and technology for secure critical infrastructure
Cyber forensics and assurance
Assuring hardware security by design
Cyber resilience for deep learning models
Artificial intelligence for cyber
Internet of Things and cloud security for smart nation
5G cybersecurity for smart nation

3.1.3 Ministry of Home Affairs

The Ministry of Home Affairs¹³ has a focus on internal affairs, much like the Home Office in the UK. The ministry has a Cyber Command with a very similar function to that of the United States Cyber Command¹⁴ and not dissimilar to the CERT in Israel¹⁵. There is a strong focus on innovation to better prepare and respond to security challenges and to strengthen partnerships with civil society within Singapore.

The ministry has more than 1,000 specialist engineers and a considerable budget approaching SING\$1 billion. Cybersecurity is relevant from two different perspectives within the Ministry of Home Affairs:

- the police and Cyber Crime Command which also covers areas such as counter-terrorism; and
- homeland security, public services, and digital assets.

MINISTRY OF HOME AFFAIRS RESEARCH INTERESTS
Forensics
Internet of Things security
Quantum cryptography and quantum key distribution
AI and cybersecurity
Blockchain

The ministry works closely with the NRF to run funding calls based around strategic challenges.

3.1.4 The Economic Development Board (EDB)

The Economic Development Board (EDB)¹⁶ is a government agency under the Ministry of Trade and Industry. It is responsible for developing and implementing strategies designed to enhance Singapore’s position as a global centre for business, innovation, and talent. The EDB has an Asian Corporate Development team that is researching how to support cyber companies.

It has played a pivotal role in attracting CISCO to set-up an Innovation Centre and Cybersecurity Centre of Excellence in Singapore. The centre aims to act as a catalyst for digital innovation that is in line with the focus areas of Singapore’s Digital Economy Framework for Action.¹⁷ Additionally, it is playing an important role in persuading others to set up their Asia Pacific Security Operations Centre in Singapore.¹⁸

¹² <https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme>.

¹³ <https://www.mha.gov.sg/>

¹⁴ <https://www.cybercom.mil/>

¹⁵ <https://il-cert.org.il/>

¹⁶ <https://www.edb.gov.sg/en/about-edb/who-we-are.html>

¹⁷ <https://www.edb.gov.sg/en/news-and-events/news/cisco-launches-first-asean-co-innovation-and-cybersecurity-centres-in-sg.html>

¹⁸ <https://www.edb.gov.sg/en/news-and-events/news/centurylink-opens-its-first-south-east-asia-security-ops-in-sg.html>

The EDB provides a number of services to assist companies who want to come to Singapore:

- local insight and access to its extensive network;
- grants and incentives; and
- legal, financial, and regulatory advisory support.

3.1.5 Enterprise Singapore

Enterprise Singapore¹⁹ is a government agency that was created as a vehicle for championing enterprise development. It is part of the Ministry of Trade and Industry.

The remit of Enterprise Singapore is to work with companies to build capabilities, innovate, and internationalise. They are also tasked with aiding the growth of Singapore as a hub for start-ups looking to establish trade within the region. They have a number of programmes for financial assistance, including:

- The Start-Up SG Founder programme²⁰ which provides access to funding, mentorship and business networks.
- The Start-Up SG Tech programme²¹ which provides early-stage funding to fast-track commercialisation of scalable in-house solutions.

Enterprise Singapore is also the national standards and accreditation body, helping to improve the standards and quality of products and services in Singapore.

In August 2018, jointly with the CSA, it formed a Coordinating Committee for Cybersecurity (CCCY)²². The CCCY aims to coordinate and facilitate the sharing of cybersecurity information in Singapore and formulate a five-year cybersecurity standards roadmap.²³ The committee is made up of representatives from government, industry and academia.

Enterprise Singapore shared their interest in strengthening ties with the UK, as evidenced by their physical presence in London.

3.1.6 Skills

The Ministry of Defence²⁴ has set up a new cyber training school that will conduct courses for specialist personnel and also help improve cyber hygiene for service members and

employees across the ministry and the Singapore Armed Forces (SAF).²⁵ They are also recruiting a considerable number of professionals to specifically work within the cybersecurity area.²⁶

Alongside the initiatives undertaken by the Ministry of Defence, the CSA is running the Singapore Cyber Youth Programme.²⁷ It is a national programme that has been created to help young people with cybersecurity. The programme is delivered in collaboration with partners from the cybersecurity industry and academia. It is aimed at students from both secondary and tertiary education. It is intended to provide young people with opportunities to make cybersecurity their career choice equipped with the right technical knowledge and skills.

Specific initiatives under this youth programme include:

- The Youth Cyber Exploration Programme²⁸, which is a boot camp delivered in collaboration with all the local Singapore polytechnics. The boot camp currently hosts around 400 students from many of the local secondary schools.
- The Student Volunteer and Recognition Programme.²⁹
- The Cybersecurity Career Mentoring Programme.³⁰

3.2 Academia

There are two main internationally recognised universities in Singapore - the NUS and NTU. NUS is ranked as the best university in Asia by QS World University Rankings and NTU is ranked second. NTU is also the world's top young university.³¹ They are ranked on the following criteria: academic reputation, employer reputation, international students and number of top academic journal citations.

3.2.1 National University of Singapore (NUS)

3.2.1.1 National University of Singapore Cybersecurity Laboratory

The National University of Singapore Cybersecurity Laboratory is intended to support R&D into new solutions and also provide a facility to test and evaluate new security solutions.

¹⁹ <https://www.enterprisesg.gov.sg/about-us/overview>

²⁰ <https://www.start-upsg.net/programmes/4894/start-up-sg-founder>

²¹ <https://www.start-upsg.net/programmes/4897/start-up-sg-tech>

²² <https://www.enterprisesg.gov.sg/esghome/media-centre/media-releases/2019/october/coordinating-committee-for-cybersecurity-formed-under-the-singapore-standards-council-to-develop-cybersecurity-standards-roadmap>

²³ <https://www.smehorizon.com/coordinating-committee-for-cybersecurity-formed-in-singapore/>

²⁴ <https://www.mindef.gov.sg/web/portal/mindef/home>

²⁵ <https://www.opengovasia.com/singapore-ministry-of-defence-opens-new-cyber-defence-school/>

²⁶ <https://www.channelnewsasia.com/news/singapore/mindef-recruit-300-cybersecurity-experts-opens-training-school-11262964>.

²⁷ <https://www.csa.gov.sg/programmes/sgcyberyouth>

²⁸ <https://www.csa.gov.sg/programmes/ycep>

²⁹ <https://www.aisp.sg/svrp.html>

³⁰ <https://www.csa.gov.sg/programmes/cybersecurity-career-mentoring-programme>

³¹ <https://www.topuniversities.com/university-rankings/world-university-rankings/2019>

The laboratory makes available a risky environment for testing and evaluating solutions. This incorporates virtual networks, vulnerabilities and malware built into the testing environment. There is also the potential to develop new products based on what is learnt from using the “risky environment”.

The laboratory provides a services architecture as the integrated risky environment which has been built in a modular fashion to enable customisation to maximise the scenarios and requirements that can be supported.³² This sort of sandbox environment is not dissimilar to the one provided by the Financial Conduct Authority in the UK for testing and evaluating financial technology (fintech) ideas and products. Over 90 projects have been supported in the laboratory in the last year, and there is a growing active community of users, including a large number of industry stakeholders.

3.2.1.2 Singtel Cybersecurity R&D Laboratory

The Singtel Cybersecurity R&D Laboratory is a corporate research facility supported by the NRF and hosted by the NUS. It was launched in 2016 and is funded by all three parties with the NRF putting up 100% of the money supported by 60% matched in-kind from both Singtel and NUS.³³ The programme of research is guided by the interests of Singtel with commercialisation in mind; they intend to enhance their services or offer new services. The key areas of interest are as follows:

R&D AREAS OF INTEREST
Predictive analytics
Network data and cloud security (privacy-preserving data sharing)
Internet of Things and industrial control systems
Future-ready cybersecurity systems – quantum technologies – quantum key distribution

Fifteen projects are running, and Singtel can fund new projects when they arise, thus providing agility and allowing Singtel to be responsive to new opportunities and build capacity. In other situations, Singtel may come to the laboratory with a specific problem seeking a solution. There are currently 72 researchers involved in the laboratory, and it has received SING\$42.7 million in funding.

Any intellectual property derived from work completed within the laboratory is wholly assigned to Singtel, and the university has the ability to licence it back on favourable terms. Promising intellectual property is translated into products and

services in Singtel, and researchers get financial remuneration when that occurs. This model for intellectual property could, however, be a disincentive for researchers as the rewards are somewhat sparse. In the instance that Singtel does not commercialise intellectual property, it may sometimes be retained by the university.

Outside of this bilateral link between the university and Singtel, there is very little international collaboration. There is, however, strong appetite, although the intellectual property model adopted may be a challenge. There is an opportunity for knowledge sharing between the UK/Singapore given the UK’s strength in structuring relationships between industry and academic institutions in a mutually beneficial way.

3.2.2 Nanyang Technological University (NTU)

3.2.2.1 School of Computer Science and Engineering (SCSE)

At the Nanyang Technological University (NTU) there are ten departments in the School of Computer Science and Engineering (SCSE)³⁴. They are collaborating with government agencies, industry and universities including some from the UK (namely: Imperial College, The University of Southampton and The University of Surrey). There is also an ongoing collaboration with BAE Systems and discussions with Rolls Royce. NTU has further international collaborations with universities in Israel and the US. The key research topics of interest are listed below.

KEY CYBERSECURITY RESEARCH TOPICS OF INTEREST
Theory, systems, practice
Cryptography, coding theory
Formal methods
Trust and resilience
Hardware security

The school commercialises 30% of its research and 40% of its work leads to a spin-off. This impressed much of the delegation; their ambition is to collaborate further with industry, with 30% of its research activity being formed with government agencies.

3.2.3 A*STAR

A*STAR³⁵ is Singapore’s government agency for economic-oriented R&D. A*STAR operates in a very similar way to the Fraunhofer Institutes in Germany and the Catapults in the UK. They aim to actively bridge the gap between academia and industry, embedding research capabilities within industry sectors.

³² <http://news.nus.edu.sg/press-releases/nus-launches-shared-national-cybersecurity-infrastructure-spur-research-and-test>.

³³ <https://www.nus-singtel.nus.edu.sg/aboutus/>

³⁴ <http://scse.ntu.edu.sg/Pages/Home.aspx>.

³⁵ <https://www.a-star.edu.sg/>

Between 2011 and 2015, A*STAR has been involved in and worked on 8,965 industry projects. This has resulted in more than SING\$1.6 billion in industry R&D spending.³⁶ A*STAR has also signed approximately 1,030 licensing agreements over the same period, of which 70% were with local SMEs.³⁷

They have a broad remit, and their funding comes directly from the NRF. They tend to focus on research activities that have an industrial perspective where customer needs are taken into account. The key R&D areas of interest are:

R&D AREAS

Detection, attribution and analysis which involves applying machine learning

Multimedia and mobile security

Forensics – stenography, steganalysis

Cyber-physical security

Data security – homomorphic, privacy-preserving analytics, cryptanalysis, blockchain security.

Security architecture assessment and solutions

The interest in collaboration is evident, and there is a clear appetite to work with the UK; however, subject to:

- Collaboration is based on assessing what the value is to Singapore.
- They prefer to work with Singapore registered entities or companies willing to hire R&D staff locally.
- There is a need to have the appropriate mechanisms to fund and support collaboration and the strategic synergies need to be present.

3.2.4 I-Trust – Centre for Research in Cybersecurity

The focus of I-Trust is on the design of secure critical infrastructure.³⁸ They are funded through strategic grants from the Ministry of Defence and the NRF. They are a National Satellite of Excellence³⁹, pursuing the design science for secure critical infrastructure.

RESEARCH AGENDA

Automation – anomaly detection

Incident response

Attestation and assessment

Digital twinning for water and electric power

Attack prevention

Novel approaches for the design of critical infrastructure

The centre has a five-year grant from the NRF to support research and experimentation in areas of secure critical infrastructure. They conduct attack/defence exercises which are open to participants from across the world and groups from the UK have taken part in the past. They are also performing technology evaluation exercises where products are evaluated by independent attack teams. The centre provides a testing and accreditation environment for software products within the context of critical infrastructure, including power and water.

Collaborative links have been established with the UK, and the delegation discovered that there is a strong appetite to collaborate further.

3.3 Industry

3.3.1 Ensign InfoSecurity

Ensign InfoSecurity⁴⁰ was founded in 2000⁴¹ and is the largest cybersecurity company in Singapore. They have approximately 500 employees and operations in other locations within Southeast Asia. Ensign is predominantly a Temasek initiative, consolidating other entities which focus on different areas/ services within the wider cybersecurity business i.e. primarily consulting, solutions and R&D labs. Ensign is closely connected with Team8 in Israel – Temasek were early investors in the Team8 fund. The remit that Ensign is working to is based on three pillars:

- to advise clients;
- architect and implement solutions;
- provide operational support.

They have a focus on providing Singapore-centric cyber threat intelligence for sectors critical to the local and regional economy. This is enabled by tools providing capabilities for automated threat hunting with an extensive malware database enhanced with signature and behavioural based discovery.

They have proprietary access to specific data and aim to gain visibility on prevailing threats and trends for holistic and pre-emptive threat mitigation on a sectoral basis. Ensign considers government-to-government information sharing to be critical. Ensign is also able to monitor IP scanning, and they profile incoming port scans and sources based on whether they are looking blindly pan-Singapore or targeting a specific business or sector.

³⁶ Choudhury, Amit Roy. "A*Star surpasses 5-year targets; industry R&D spend exceeds S\$1.6b". The Business Times. 16 June 2017.

³⁷ https://en.wikipedia.org/wiki/Agency_for_Science,_Technology_and_Research

³⁸ <https://itrust.sutd.edu.sg/>

³⁹ <https://itrust.sutd.edu.sg/hsoe-destsci/>

⁴⁰ <https://www.ensigninfosecurity.com/>

⁴¹ <https://www.crunchbase.com/organization/ensign-infosecurity#section-overview>

The R&D labs are focused on developing new bespoke solutions to address current and emerging threats. Ensign allocates 30% of its resources to R&D.⁴²

RESEARCH INTERESTS

Vulnerability research focused on the more critical systems as defined by their customers

Data analytics – advanced threat detection, network behavioral analytics and tradecraft knowledge

Threat research and intelligence

Advanced sensors technologies

5G and cybersecurity

3.4 Collaborative Efforts

3.4.1 Singapore Cybersecurity Consortium

The Singapore Cybersecurity Consortium⁴³ forms part of the effort under the National Cybersecurity R&D Programme.⁴⁴ It represents another initiative where industry, academia and government come together to support the National Satellites of Excellence⁴⁵. Their aim is to develop and bring together local cybersecurity research strengths in domains that are of national interest.

NATIONAL SATELLITES OF EXCELLENCE FOCUS AREAS

Trustworthy software systems

Design science and technology for secure critical infrastructure

Mobile systems security

Cloud security

The consortium is funded by the NRF and cybersecurity companies can apply for consortium membership. The consortium provides seed funding⁴⁶ to develop proofs-of-concept in collaboration with academia. This grant is for the advancement of new cybersecurity technologies and innovative ideas, which seek to address gaps in the cybersecurity landscape whilst strengthening Singapore’s cybersecurity capabilities against present and future threats. Companies that are members of the consortium are able to jointly submit a proposal with academia/research institutes or public agencies.

⁴² <https://www.ensigninfosecurity.com/the-ensign-difference>.

⁴³ <https://sgcsc.sg/>

⁴⁴ <https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme>

⁴⁵ <https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme>

⁴⁶ <https://sgcsc.sg/research.html>

4. Coming to Singapore

At a commercial level, the potential market for cybersecurity services in the ASEAN region is projected to almost triple over the next five to six years.⁴⁷ The ASEAN markets are all different in terms of maturity and focus. They all offer a different level of cybersecurity readiness across both government and business. Singapore represents the most mature market within the region and is experiencing significant growth.

Singapore is keen to attract companies and individuals from overseas who can help to accelerate the efforts within Singapore to become a global leader in cybersecurity. Within this context, Singapore provides a number of support mechanisms, incentives and funding. These come from the likes of EDB, Enterprise Singapore and ICE71.

Relationships and partnerships are critical for success in Singapore and the wider region. Brand recognition, even for a big global multinational, can be a challenge in Singapore. Singtel is a huge competitor, and borderline monopoly and Singaporeans generally prefer to put Singapore first over large multinational providers if providing a similar service or product.

The view from start-ups like Right Hand Cybersecurity⁴⁸, is that Singapore represents a unique opportunity to reach an emerging market experiencing considerable growth and digital transformation.

4.1 Start-up and Investor Landscape

In Singapore, programmes like Block71 (ICE71)⁴⁹ and the Early Stage Venture Fund⁵⁰, are compelling examples of initiatives to strengthen talent and innovation among cybersecurity start-ups. Singaporeans are traditionally risk-averse and working in or founding a start-up is still seen as an uncertain career path. Working in a bank, becoming a doctor or a lawyer are seen as safer options leading to success and stability. The cultural dynamic, therefore, inhibits an inflow of talent into the start-up sector, which is a necessary component of ecosystem maturity.

Singapore seems to increasingly be looking to Israel to learn how to implement and successfully build an entrepreneurial ecosystem. Israel's rise as a global cybersecurity superpower has been remarkable – it now has the highest density of tech start-ups in the world and attracts more venture capital

dollars per capita than any other country. The report from the Expert Mission to Israel in June 2018 provides a good overview of the Israeli cybersecurity innovation landscape.⁵¹ From heritage and geography, both Singapore and Israel contend with scarcity and limitations in size, prompting strong initiatives to develop technology and cybersecurity competence for survival and competitive advantage.⁵²

For Singapore to progress and advance to the levels reached by Israel, it will have to develop a self-sustaining ecosystem, where the government, education system, business, start-up community, and public sector work in unison to continually improve cybersecurity capabilities. This is beginning to happen with closer ties developing between government, industry and research as noted in Section 3 of this report.

The investor landscape in Singapore is improving but still has some way to go. Global funds have recognised the potential of the region and have started to build their teams in the region to identify, invest and support companies operating in both Singapore and further afield across ASEAN. Investors in Singapore are typically risk-averse. The angel investor landscape in Singapore is also growing but has some way to go before it catches up with the UK and Israel.

4.2 ICE71

The Innovation Cybersecurity Ecosystem at Block71 (ICE71) is the region's first cybersecurity entrepreneur hub. ICE71 is a partnership between Singtel Innov8 which is the venture capital arm of the Singtel Group, and the NUS, through its entrepreneurial arm NUS Enterprise.⁵³

The mission of ICE71 is to strengthen the cybersecurity ecosystem in Singapore and the wider ASEAN region. They are looking to do this by attracting and developing capabilities and deep technologies that will help mitigate and minimise the impact of the rapidly increasing cybersecurity risks in the region. ICE71 is supported by the CSA and IMDA. ICE71 runs

⁴⁷ ASEAN Market Insights, AUSTRADE 2018.

⁴⁸ <https://right-hand.ai/>

⁴⁹ <https://ice71.sg/>

⁵⁰ <https://www.nrf.gov.sg/funding-grants/early-stage-venture-fund>

⁵¹ https://admin.ktn-uk.co.uk/app/uploads/2019/03/216_KTN_Cybersecurity_Israel_v4.pdf

⁵² <https://sbr.com.sg/financial-services/commentary/can-singapore-become-latest-and-greatest-regional-cybersecurity-hub>

⁵³ <https://ice71.sg/>

a range of programmes designed to support cybersecurity individuals and start-ups from idea development to the creation, acceleration and scaling of cybersecurity start-ups:

- ICE71 Inspire – a programme aimed at the idea stage and at supporting those interested in the entrepreneurial track.
- ICE71 Accelerate – a 13-week programme aimed at start-ups who have an MVP and have generated some interest in their respective target market(s). The support provided includes mentorship, training, office space, funding (approximately £15K) and a network.
- ICE71 Scale aims to help international and local companies grow their business in Singapore and the ASEAN region. Companies taking part, take up residency at ICE71 with a view to establishing a headquarters for their Asia Pacific operations.

The Inspire and Accelerate programmes are run by CyLon, which is Europe’s leading and very first accelerator programme in cybersecurity. The experience held by CyLon, combined with ICE71’s regional expertise, provides start-ups with the support and advice required to launch and grow a successful cybersecurity business in Singapore and potentially across the wider ASEAN region.

4.3 Enterprise Singapore

Enterprise Singapore provides access to investment for new companies:

- The Start-up SG Equity scheme is one which sees the government co-invest with independent and qualified third party investors into eligible start-ups.⁵⁴
- SEEDS Capital co-invests in scalable, innovative start-ups with strong intellectual property.⁵⁵
- A government-linked fund, EDBI⁵⁶ invests in promising companies across diversified industries.⁵⁷

4.4 Singtel Innov8

Singtel Innov8⁵⁸, the venture capital arm of the Singtel Group, invests in and partners with innovative tech start-ups worldwide. It has a fund size of US\$250 million and its own set

of decision making, approval and funding processes. Beyond funding, Singtel Innov8 is a gateway for start-ups to tap into the resources and expertise of the Singtel Group while enabling the group to gain access to emerging technologies. Singtel Innov8 focuses its investments on technologies and solutions that can lead to quantum changes in network capabilities, next-generation devices, digital services and enablers to enhance customer experience. Headquartered in Singapore, Singtel Innov8 has five offices in the ASEAN region as well as in San Francisco and Tel Aviv.

It operates as an Evergreen Fund, which means profits from successful exits are re-invested back into the fund. The investments tend to focus on mature start-ups i.e. Series A onwards. Singtel Innov8 have made 97 investments, and in 23, they were the lead investor. They have made 26 successful exits⁵⁹. The geographical dispersion of these investments is:

- 60% American investments
- 15% Israel
- 25% across the rest of the world.

Singtel Innov8 has formed strong alliances with Telefonica⁶⁰, Orange and Deutsch Telekom⁶¹ which provides global coverage and vision to the fund. There are further alliances with SoftBank and AT&T⁶² looking specifically at cybersecurity.

Scouting is guided explicitly by innovations that can help Singtel strategically and or enhance their service offerings in the market. The scouting strategy is, therefore developed on the basis of what the corporate entity wants. On occasion, they also make small investments on high risk, high reward ideas.

There is a real commitment within Singtel Innov8 to act as an enabler within the Singtel Group, providing insight and education on emerging technologies and capabilities.

⁵⁴ <https://www.start-upsg.net/programmes/4895/start-up-sg-equity>

⁵⁵ <https://www.enterpriseg.gov.sg/financial-assistance/investments/investments/seeds-capital/overview>

⁵⁶ <https://www.edbi.com/>

⁵⁷ <https://www.edbi.com/>

⁵⁸ <http://innov8.singtel.com/>

⁵⁹ <https://www.crunchbase.com/organization/singtel-innov8#section-exits>

⁶⁰ <https://www.telefonica.com/en/>

⁶¹ <https://www.telekom.com/en>

⁶² <https://www.att.com/>

4.5 Temasek

Temasek⁶³ was founded in 1974 as a commercial investment company which is wholly owned by the Singapore government but operates independently and is not directed by the government. They have approximately 800 staff and 11 offices globally.

The primary source of funds comes from returns made on investments – as such, they are an Evergreen Fund. Temasek has an independent board of governors with no participation from personnel who are active office holders within the Singaporean government. They have built a venture capital fund network, including, Team8 based in Israel, Teneleven Ventures⁶⁴ linked to KKR⁶⁵, and Clearsky⁶⁶ linked to Blackstone⁶⁷. They were lead investors in the first and second funds of Team8. The Temasek portfolio is valued at a staggering S\$313 billion.

Before the year 2000, Temasek focused primarily on investments within Singapore. However, they have since seen opportunities elsewhere and have shifted their attention to the rest of Asia and the world.

In terms of their investment portfolio, financial services and telecoms dominate although they are now investing in consumer products and services, transportation and life sciences. Through their partners, they have invested in IP commercialisation. In the UK that includes working with the IP Group⁶⁸ in Cambridge and Oxford Sciences Innovation⁶⁹.

As well as making direct investment (typically at the Series B stage and beyond), Temasek has also taken Limited Partner (LP) positions in a number of funds to diversify their portfolio. Temasek is looking for yielding assets delivering dividends and divestments - and this is likely to increase. There is an opportunity for the UK to offer Temasek access to larger, more mature alternative assets.

4.5.1 The Global Cybersecurity Platform

Temasek is developing a Global Cybersecurity Platform, aiming to bring together stakeholders to address key issues, including:

- Protecting the portfolio of investments in Singapore - the platform will provide an end-to-end set of services offering solutions as a managed security service.
- Providing venture capital funds with insight and access to the most disruptive technology in the sector.
- Partnership building to facilitate the transfer of insight, technology and capability e.g. secondments, training and joint R&D collaboration.
- Identifying and investing in and/or partnering with the most cutting-edge innovative companies.

Temasek is interested in hosting the platform in the UK, namely because of the strong talent base and breadth of technology opportunities. This might offer opportunities to invest in UK technology and to gain a wider portfolio coverage in Europe where they currently have no involvement from an investment perspective. They are particularly interested in building up their services - they are looking for trusted advisors to help their portfolio companies - "CISO as a service". Investments in product companies will be highly selective. From discussions during the mission, it was apparent that Temasek had a greater interest in services.

The regulatory landscape in the UK and across Europe is interesting for them, and they are keen to better understand the impact of GDPR as part of their decision-making process. GDPR can be seen as highlighting the importance of enterprise security, which presents an opportunity for product sales, further innovation, and R&D given the heightened interest in data security.

⁶³ <https://www.temasek.com.sg/en/index.html>

⁶⁴ <https://www.1011vc.com/>

⁶⁵ <https://www.kkr.com/>

⁶⁶ <http://www.clear-sky.com/>

⁶⁷ <https://www.blackstone.com/>

⁶⁸ <https://www.ipgroupplc.com/>

⁶⁹ <https://www.oxfordsciencesinnovation.com/>

5. Collaboration

Collaboration brings challenges, but where individuals, organisations (public and private) or countries have shared history, goals and vision, there is always potential to achieve more together by maximising the impact of shared expertise, knowledge and capabilities. In the case of UK and Singapore, the shared history dates back to 1819 when Sir Stanford Raffles founded a trading port which some have argued set the stage for modern-day Singapore.⁷⁰

The UK is Singapore's fifth-largest European trading partner and sixth-largest investor globally. There are more than 4,000 British companies in Singapore, including Rolls-Royce, GlaxoSmithKline, BAE Systems, BT and Dyson, all of whom have contributed significantly to innovation.⁷¹

5.1 Existing UK-Singapore Collaboration

Collaboration has already featured in the close relationship between the UK and Singapore. Some of the specific collaborations on cybersecurity that have come to fruition include:

Earlier in 2019, the Monetary Authority of Singapore (MAS), the Bank of England and the UK Financial Conduct Authority announced their commitment to working together on improving cybersecurity in financial institutions. The collaboration is aimed at identifying effective ways to share information and exploring the potential for staff exchanges. Given that both Singapore and the UK are hosts to two of the world's leading financial centres and both have a thriving fintech ecosystem, this collaboration makes natural sense for both jurisdictions.⁷²

The UK National Cybersecurity Centre (NCSC) and the CSA have signed a partnership focused on IoT security for consumers. Both countries will share and exchange initiatives, approaches, information, and experiences to promote the implementation of good practices based on global IoT industry standards.⁷³

Enterprise Singapore governs the national standards of Singapore and as such works alongside the UK's British Standards Institution on international standards through international bodies such as ISO, IEC and IEEE. Both countries work together within the ISO/IEC Joint Technical Committees that work on standards for information security, governance, business continuity and data privacy.

In June 2018, Singapore and the UK signed a Memorandum of Cooperation (MoC) on Cybersecurity Capacity Building,⁷⁴ It was jointly signed by Singapore's Minister for Foreign Affairs and the UK Secretary of State for Digital, Culture, Media and Sports.

In July 2015 the CSA signed a Memorandum of Understanding (MOU) on cybersecurity cooperation with the Cabinet Office in the UK, formalising both countries commitment to ensuring a secure cyberspace that supports innovation as well as economic and social development for both countries.⁷⁵

The academia in Singapore and the UK are continuing to collaborate on R&D on an informal basis where the research interests are already aligned and where relationships between individuals or groups already exist.

Under the EUREKA programme, there was a funding call in 2019 for a share of £1 million for partnerships between the UK and Singapore to develop disruptive and game-changing innovations in a variety of fields.

In 2015 the NRF, the UK Cabinet Office and EPSRC funded collaborative research projects in cybersecurity between academia in Singapore and the UK. The funding call welcomed proposals addressing shared challenges in⁷⁶:

- Intrusion: malware, exploits, intrusion detection and protection.
- Data analytics: algorithms, machine learning, privacy, trust, and personal/aggregated data issues (big data).
- Human factors: usability, behaviours, incentives, and more general economic, social and legal concerns.
- Policy aspects: issues that directly affect policy, government or business. Includes best-practices (e.g. bring your own device), ownership (e.g. copyright, digital rights management), regulation and compliance.
- Sectors and applications (e.g. IoT): targets the concerns of particular sectors or applications. Includes general areas such as healthcare and cities, to specific issues, e.g. smart cities, and detecting extremist activity.

5.2 Challenges

- R&D partnerships and collaborations between cyber start-ups are challenging because as young companies, they are still vulnerable with divergent strategies and different investor pressures.
- Cybersecurity companies in Singapore, as in other places, are primarily focused on sales and expanding their routes to new markets. This is even more critical when taking into account the small domestic internal market. As such, it means that collaboration on innovation is not at the forefront of their strategic agenda.
- Doing business in Singapore and the wider region is all about building relationships and partnerships in order to gain customer trust and long-term acceptance within the local market. The same is true of any long-term strategic collaborations, and this could be challenging for any UK organisations which have not spent the time to build a local network of contacts and relationships which could well be a pre-requisite to any successful tangible collaborations.
- Tangible collaborations on innovation in cybersecurity across multiple jurisdictions can bring about complexity from the divergent regulatory and legal frameworks governing industry sectors locally. This can bring about conflicting interests and requirements which could lead to results of innovation projects not really delivering in full for either party.

⁷⁰ Chew, Ernest C T, and Edwin Lee. A History of Singapore. Singapore: Oxford University Press, 1991.

⁷¹ <https://www.straitstimes.com/singapore/singapore-and-uk-share-a-rich-and-enduring-friendship-based-on-long-history-halimah>

⁷² <https://www.bankofengland.co.uk/news/2019/june/mas-and-uk-financial-authorities-announce-collaboration-on-cyber-security>

⁷³ <https://dig.watch/updates/uk-and-singapore-sign-partnership-consumer-iot-security>

⁷⁴ <https://www.opengovasia.com/singapore-and-uk-to-cooperate-on-cybersecurity-capacity-building/>

⁷⁵ <https://www.csa.gov.sg/news/press-releases/singapore-and-the-uk-commit-to-work-together-to-ensure-a-secure-cyberspace>

⁷⁶ <https://epsr.org.uk/funding/calls/singaporeukcybersec/>

Annex 1

List of UK Participants

Assentian Partners

British Telecommunications

Department for Digital, Culture, Media and Sport (DCMS)

Digital Shadows

Innovate UK

Knowledge Transfer Network

Level39

Mercia Asset Management PLC

UCL (University College London)/Research Institute for The Science of Cybersecurity (RISCS)

List of Singapore Participants

A*STAR

The Cybersecurity Agency (CSA)

Economic Development Board (EDB)

Ensign InfoSecurity

Enterprise Singapore

ICE71

I-Trust – Centre for Research in Cybersecurity

Nanyang Technological University (NTU)

National University of Singapore (NUS)

Singapore Cybersecurity Consortium

Singapore National Research Foundation

Singtel Innov8

Temasek

