Policy Analysis: Singapore's Public-Private Partnerships for Cybersecurity in the Critical Infrastructure Sectors — Challenges and Opportunities

In 2000, the United States government established the Partnership for Critical Infrastructure Security (PCIS), a partnership framework between the government and private sector that aimed to improve the protection and resilience of America's critical infrastructure sectors. The public-private partnership (PPP) for cybersecurity was the first of its kind, and was widely seen as a landmark move.

The significance of that move would come several years later, when cyber attacks in several countries highlighted the importance of protecting national essential services and pushed the concept of cyber warfare to the front of many nations' consciousness. Most nations now realise how vulnerable national essential services can be to a cyber attack, thanks to the widespread adoption of infocomm technologies in critical infrastructures. In June 2016, NATO officially recognised cyberspace as an "operational domain" — an area in which nations must plan for attack and defence.[1]

Since the PCIS, more of such initiatives have been set up around the world to address the growing demand for cybersecurity. Such partnerships have become essential given the extent of privatisation, deregulation and globalisation in many countries' critical infrastructure sectors. While their effectiveness may differ depending on each country's unique political, economic, social, technological and legal environments, PPPs arguably have a value proposition, at least at face value, as they leverage on the strengths of both public and private sectors. This is especially true in Singapore, whose aggressive push to be the world's first Smart Nation makes the need for a safe and secure digital environment even more critical.[2]

This case study examines Singapore's strategy and use of PPPs for tackling the issue of cybersecurity in its critical infrastructure sectors. It also suggests enhancements and highlights areas where such partnerships could help raise cybersecurity standards in these sectors.

As cybersecurity strategy and the details of PPPs pertaining to critical infrastructure sectors are often sensitive, key stakeholders are understandably reluctant to speak openly about specifics. While some of the information presented in this case study is based on informal discussions with representatives familiar with such arrangements, the case study will not provide details of these representatives.

---

[1] "NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit | CCDCOE," 2016. https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html.
[2] Kwang, Kevin. "National Cybersecurity Strategy Aims to Make Smart Nation Safe: PM Lee." *Channel NewsAsia*, October 10, 2016. http://www.channelnewsasia.com/news/singapore/national-cybersecurity-strategy-aims-to-make-smart-nation-safe/3193210.html.

This policy analysis was written by Lim Wei Chieh under the guidance of Hawyee Auyong and Tara Thean, Lee Kuan Yew School of Public Policy (LKY School), National University of Singapore and has been funded by the LKY School. The case does not reflect the views of the sponsoring organisation nor is it intended to suggest correct or incorrect handling of the situation depicted. The case is not intended to serve as a primary source of data and is meant solely for class discussion.

Cybersecurity Protection: How Singapore Protects Its CII

Certain services are considered essential to Singapore's societal, economic and national security. According to the Computer Misuse and Cybersecurity Act (2013)[3], these are defined as "services directly related to communications infrastructure, banking and finance, public utilities, public transportation, land transport infrastructure, aviation, shipping, or public key infrastructure; or emergency services such as police, civil defence or health services".

These essential services are supported by assets commonly referred to as Critical Infrastructure (CI), which are dependent on the proper functioning of integral information and communication infrastructure, also known as Critical Information Infrastructure (CII). For example, in the essential service of electric power generation, the CI is the power plant, and the CII is the information and communications systems running the plant.

The risk of cyber attacks on CII has increased as a result of two trends. The first is the growing adoption of infocomm technologies by private CI companies as part of efforts to increase productivity and reduce cost, which introduces more weaknesses and vulnerabilities into the CII, as well as more complexities in protection. The second is the greater use of more "open" technologies in place of proprietary control and management systems,[4] which exposes systems to a wider pool of potential attackers.

Such concerns drive many of the high-level plans and programmes that Singapore has set up in the context of infocomm security. Heavy emphasis was placed on the protection of Singapore's CIIs by the Republic's second Infocomm Security Masterplan (2005-2007), while the main aim of the Cyber Security Agency (CSA), set up in April 2015, was to develop cybersecurity, protect CIIs, and coordinate national efforts against large-scale cyber incidents. When the Cyber Security Strategy was launched in October 2016, one of its key pillars was strengthening the resilience of CIIs. And a key area of the latest National Cyber Security Masterplan 2018 involves enhancing the security and resilience of Singapore's CIIs by improving cross-sector responses to cyber attacks, conducting cyber security exercises, and assessing the security and resilience of high-priority CIIs in each sector.

Privatisation, Deregulation, Globalisation and the Challenges for CII Cybersecurity

As we have seen, the protection of CII has become more complex and challenging because of the increasing use of infocomms and "open" technologies. This challenge is intensified by three key global market forces: privatisation, deregulation, and globalisation.

Privatisation and deregulation in the CI sector has placed an ever-increasing proportion of CI and CII assets in the hands of the private sector, while globalisation has widened

---

[3] Computer Misuse and Cybersecurity Act. Singapore. Accessed January 16, 2017. http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3A8a3534de-991c-4e0e-88c5-4ffa712e72af Status%3Ainforce Depth%3A0;rec=0;whole=yes.

[4] Carr, Madeline. "Public – Private Partnerships in National Cyber-Security Strategies." International Affairs 1, no. 1 (2016): 190–209. doi:10.1111/1468-2346.12504.

the ownership of these assets to foreign players as well. In the United Kingdom, 80 percent of CI[5] is under private sector control. The figure is even higher in the United States at 90 percent.[6]

This means that today, governments are increasingly reliant not only on the private sector for CII protection, but also on an institutionally-fragmented network of private organisations with competing goals and interests.[7] At the same time, the interdependence of CII today also means that both governments and companies are operating in an environment in which shared risks need to be controlled through shared responsibility and joint risk management.[8]

The main challenge that governments face in protecting CII is rooted in the fact that with privatisation, ownership of an essential service and the responsibility for service delivery and reliability now lie in with a private owner. While some may argue that self-preservation will motivate companies to invest sufficiently in cybersecurity, the reality of the competitive market environment is that it tends to drive a short-term, revenue-focused approach rather than a long-term view of business continuity.[9]

So although governments and private owners have a common goal to keep a CII secure, the motivation to do so is different. Governments view essential services as a public good and therefore seek to ensure national security and mitigate the massive societal impact of a kinetic cyber attack — an attack in cyberspace that has a physical impact. Private owners and operators, on the other hand, are focused on avoiding the potential financial and reputational costs of a security breach. They are unlikely to accept the responsibility or liability for national security as their decisions will be based on a profit-maximising framework. This means that companies will neither invest in CII protection beyond their cost-benefit analysis to accommodate the public interest nor consider the full social costs; they will accept responsibility for securing CII only to the extent that they can avoid the cost of a cyber incident and still be profitable.[4]

This difference means that governments and companies will hold different views on the measurement of success and risks of cybersecurity, even in a successful PPP. The private sector will accept a certain level of risk and will invest in cybersecurity only to the point where the cost of implementation does not exceed the cost of a security incident. The public sector, in contrast, will have a lower risk acceptance level and thus be willing to invest beyond the cost of a security incident.

As such, the cybersecurity of CII will be insufficient if we rely solely on market forces. Most industries would prefer the state to take a self-regulatory approach, but the

---

[5] Orsula, Anna-Maria. “National Cyber Security Organisation: United Kingdom,” 2015. https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_UK_032015_0.pdf.
[6] Charles, Deborah. “NSA Chief Says U.S. Infrastructure Highly Vulnerable to Cyber Attack | Reuters.” Reuters, June 12, 2013. http://www.reuters.com/article/us-usa-cybersecurity-idUSBRE95B10220130612.
[7] de Bruijne, Mark, and Michel van Eeten. “Systems That Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment.” Journal of Contingencies and Crisis Management 15, no. 1 (March 2007): 18–29. doi:10.1111/j.1468-5973.2007.00501.x.
[8] Dunn Cavelty, Myriam, and Manuel Suter. “Public-Private Partnerships Are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection.” International Journal of Critical Infrastructure 4, no. 2 (2009): 179–87.
[9] Givens, Austen D, and Nathan E Busch. “Realizing the Promise of Public-Private Partnerships in U.S. Critical Infrastructure Protection.” International Journal of Critical Infrastructure Protection 6, no. 1 (2013): 39–50. doi:10.1016/j.ijcip.2013.02.002.

effectiveness of this approach would require governments to rely on companies' voluntary adoption of best practices, greater collaboration within the sectors, and voluntary cybersecurity investment on the part of companies to meet national security needs. Either government-funded incentives or government intervention in the form of oversight, regulation and partnership are needed to close this gap. But this can give rise to several dilemmas.

First, while some form of government intervention is widely accepted as unavoidable given the potential societal costs of CI disruptions and failures, any moves made by the state to ensure cybersecurity as a public good may be seen as distorting market forces and negating the benefits of privatisation and globalisation. This is especially so as CI sectors often form the foundation of a nation's economic success.[8]

Second, governments have to tread the fine line between ensuring national security and respecting private CI owners' need to secure their businesses. Governments cannot be seen to be passing on their responsibility for national security – a core obligation of the state — to the private sector.[4] At the same time, they also cannot be seen to be taking on the responsibility that private enterprises hold in providing secure and reliable services to their customers, which may well include foreign nations and commercial entities.

To understand how Singapore deals with such dilemmas and manages the accountability structures of its CI sectors, we need to take a deeper look at how the country's political and economic environment has been shaped by privatisation, deregulation and globalisation, and see how this affects its efforts to ensure cybersecurity.

CII Cybersecurity in Singapore: The Government's Role

After gaining its independence in 1965, Singapore relied on state-led development in various key sectors to boost its economy, establishing state-owned enterprises known as Government-Linked Companies (GLCs) as part of its industrialisation plan. This injection of state capital helped to compensate for the lack of private sector funds and expertise.[10] In 1974, the government set up investment company Temasek Holdings to manage these assets so that the Ministry of Finance could continue to focus on its core policymaking and regulatory roles.

While strong government involvement was crucial at the nation's early stages of growth, a recession in 1985 demonstrated the need for deregulation and privatisation, so that the private sector, operating under market forces, would drive efficiency and productivity to provide greater economic growth. Over the next decade, some 40 GLCs were privatised, along with statutory boards[11] and CIs, starting with the telecommunications sector. The extent of privatisation and deregulation, however, has been substantially different across the CI sectors, as can be seen from an examination of Temasek Holdings' stake in key companies in the aviation, electricity, banking and telecommunication sectors (Table 1).

[10] Ramirez, Carlos D., and Ling Hui Tan. "Singapore Inc. Versus the Private Sector: Are Government-Linked Companies Different?" IMF Staff Papers 51, no. 3 (2004). https://www.imf.org/External/Pubs/FT/staffp/2004/03/ramirez.htm.
[11] Foo, Choy Peng. "Committee Names 41 Companies for Privatisation." Business Times, March 14, 1987. http://eresources.nlb.gov.sg/newspapers/Digitised/Article/biztimes19870314-1.2.4.

Table 1. Temasek Holdings' Stake in Key Companies

Sector	Company	Shareholding (%)[a]
Aviation	Changi Airport Group	100[b]
	Singapore Airlines	56
	ST Aerospace	50[c]
	SATS	43
Electricity (Transmission)	Singapore Power	100
Electricity (Generation)	Sembcorp Cogen	49[d]
	Keppel Cogen	10[e]
	Senoko Energy	0
	Tuas Power	0
	YTL PowerSeraya	0
Banking	DBS	30
	OCBC	0
	UOB	0
Telecommunications	SingTel	51
	StarHub	56
	M1	19
	TPG Telecom	0[f]

[a] *Shareholding (%) (rounded) as at 31 March 2016*
[b] *100% owned by Ministry of Finance and yet to be transferred to Temasek Holdings*
[c] *100% Subsidiary of ST Engineering (which is 50% owned by Temasek Holdings)*
[d] *100% Subsidiary of Sembcorp (which is 49% owned by Temasek Holdings)*
[e] *49% owned by Keppel Corporation (which is 21% owned by Temasek Holdings)*
[f] *Licence awarded in December 2016*

Table 1 clearly shows that privatisation of the CI sectors has taken place at a varying pace:

- The aviation sector is still very much under public sector ownership and control.
- Electricity generation is largely deregulated and a significant number of operators are foreign companies. Ownership of the generation companies, however, still lies in the hands of Singaporean conglomerates, while the government retains full ownership of the transmission system needed to distribute electricity to consumers.
- The banking sector is highly privatised and public sector ownership is limited.
- The telecommunications sector remains majority-owned by the public sector.

The different levels of public sector ownership across the CI sectors means that the sectors cannot handle cybersecurity uniformly. For companies that are fully- or majority-owned by the government, the industry generally holds the view that

cybersecurity can be fully implemented to a level necessary for national security, since the companies have access to public funds. For certain private owners or operators where the state is the sole or a significant customer, extensive cybersecurity can also be implemented as the customer can dictate these requirements in line with general market rules.

In certain situations, national and commercial interests may even be aligned, with both public and private sectors sharing a similar threshold for cyber risk acceptance. According to a representative in Singapore's banking sector who is familiar with the matter, government demands for additional measures have so far been in line with the banking sector's own cyber risk management requirements.

For privately-owned companies and operators in the CI sector, we have seen how government intervention is inevitably necessary to ensure cybersecurity when the public sector has no or limited managerial control of these sectors – which is the case with essential services that are fully- or partially-owned by private entities in Singapore. In the Republic, this intervention takes the form of tough cybersecurity laws enacted at the national level, as well as strict regulations implemented at the sectoral level.

At the national level, Singapore has enacted the Computer Misuse Act 1993, which was updated in March 2013 and renamed the Computer Misuse and Cybersecurity Act to strengthen measures to make the country's CII more robust and resilient to cyber threats. It includes a key provision for the state to direct "a person or an organisation to take measures necessary to prevent, detect or counter cyber attacks" when it is deemed "necessary for the purposes of preventing, detecting or countering any threat to the national security, essential services or defence of Singapore or foreign relations of Singapore".[3] Plans are also being made for a new Cybersecurity Act to be introduced in 2017, to give the Cyber Security Agency greater powers to secure the nation's CIIs and require CII owners and operators to secure their systems and networks.

At the sectoral level, the Critical Infocomm Infrastructure Surety Assessment project was launched in 2006, and the Cybersecurity Readiness Maturity Assessment programme in 2012. These programmes help the state and operators to assess and improve the cybersecurity readiness of CIIs.

However, the experience of other mature economies has shown that tough cybersecurity laws may not be the best approach, as they are dependent on various political and economic factors. In the United States, for example, the private sector often views government requirements on cybersecurity measures as unwelcome regulation that will hamper innovation. Many companies also feel that these regulations would impose substantial costs which would affect their profitability. Further, they see the regulations as unfair and inappropriate as they believe cybersecurity should be considered the sole responsibility of the public sector. As a result, the American government has largely avoided mandatory regulation in the face of private sector opposition.[12]

The alternative, then, is for the government to intervene through partnerships. Over the years, both public and private sectors have come to recognise that effective cyber

[12] Etzioni, Amitai. "The Private Sector: A Reluctant Partner in Cybersecurity." Georgetown Journal of International Affairs, no. International Engagement on Cyber IV (2014): 160. https://icps.gwu.edu/private-sector-reluctant-partner-cybersecurity.

defence for CII can be achieved only through collaboration within and across sectors. This has given rise to many nations pursuing cybersecurity strategies that emphasise the need for some form of public-private partnerships (PPPs).

This has been especially true in Singapore, where industry partnership has been a recurring theme since the first Infocomm Security Masterplan was introduced in 2005. It is worth noting at this point that PPPs are intended to complement, not replace, legislation and regulation by addressing areas that are not fully covered in either breadth or depth by compliance requirements. Such partnerships should not be seen as a means of reducing the need for legislation and regulation, as has been clearly seen in the case of Singapore.

PPPs in Singapore: How They Work

Fundamentally, a PPP is an arrangement between the public and private sector to pool resources to achieve a shared goal which otherwise cannot be successfully or optimally attained solely by either party.[8]

It is important to understand the distinction between privatisation and a PPP. In privatisation, a public service owned and operated by the government is fully or substantially divested to the private sector, which then assumes ownership and responsibility for the service. The government retains indirect control through regulation and licensing to ensure optimal delivery of the public service. In a PPP, however, the government acquires the public service from the private sector on behalf of the public and retains final responsibility for the service.

Public Sector Owner and Operator	**Public-Private Partnerships**	**Private Sector Owner and Operator**
Goal	▪ Optimise public service by making full use of different roles and strengths of the public and private sectors.	▪ Enhance public service by making full use of market forces to drive positive practices and behaviour.
Characteristics	▪ Long-term agreement (more than 25 years) built on shared goals, risks, resources, rewards and decision making. ▪ Public sector acquires services from the private sector on behalf of the public. ▪ Government retains	▪ Full divestiture or transfer of all or substantial public service assets to the private sector. ▪ Private sector assumes ownership and responsibility for the service. ▪ Government retains indirect control

ultimate responsibility for the public service.	through regulation and licensing to deliver the service to the public.

In Singapore, the official definition of a PPP as issued by the Ministry of Finance is based on a long-term partnering relationship between the public and private sectors to deliver services to the public. Underlying this partnership is the principle of bringing together the expertise and resources of the public and private sectors to provide services to the public at the best value for money.[13] A key objective is to allow the government to focus on its core responsibilities of policy-making and regulation by transforming its role as a service provider to that of a buyer.

The PPP model was first used by the Public Utilities Board in 2003 to build the Tuas Desalination Plant. Its success prompted the Ministry of Finance to introduce PPPs as a form of procurement under the Best Sourcing framework in 2004, and to promote and establish guidelines for structuring and managing PPP projects.[14] Most of Singapore's PPPs are based on variations of the Design-Build-Finance-Operate (DBFO) model, in which all parties agree to share risks, resources and decisions in delivering public service projects. One example is the Sports Hub PPP, in which a private-sector consortium has a 25-year contract to manage the S$1.3 billion facility at a cost of S$193.7 million to the government.

Unlike other PPPs, this DBFO project has seen mixed results, with funding difficulties, delays in completion, maintenance issues and higher costs, raising questions over whether or not the PPP has indeed delivered services to the public at the best value for money.[15] [16]

Cybersecurity PPPs in Singapore: A Deeper Look

In 2013, the United States' General Accountability Office (GAO) released a report noting that the private sector had not fully engaged with the government's cybersecurity strategy and had not done enough to protect critical infrastructure against cyber threats. The report suggested that the government expected the private sector to commit to (1) participating in information sharing programmes; and to (2) executing government plans and recommendations. The expectation here was that the private sector should respond adequately to avoid regulation, which would burden both public and private sectors with the cost of administering and managing regulatory compliance.[4]

Do PPPs for cybersecurity in Singapore face similar challenges as those in the US? Do the different parties hold radically different perspectives when they call on the other side to "work together", and if so, how do they deal with these differences?

---

[13] "Government Procurement Process." Accessed January 20, 2017. http://www.mof.gov.sg/Policies/Government-Procurement/Procurement-Process.
[14] PUBLIC PRIVATE PARTNERSHIP HANDBOOK VERSION 2. Ministry of Finance, 2012. http://www.mof.gov.sg/Portals/0/Policies/ProcurementProcess/PPPHandbook2012.pdf.
[15] Chow, Jermyn. "NDP 2016 at Sports Hub to Cost $39.4m, Singapore News & Top Stories - The Straits Times." The Straits Times, March 1, 2016. http://www.straitstimes.com/singapore/ndp-2016-at-sports-hub-to-cost-394m.
[16] Chua, Siang Yee. "Football: No Kallang Home for Lions?" The Straits Times, January 13, 2017. http://www.straitstimes.com/sport/football/no-kallang-home-for-lions.

One of Singapore's first major PPP projects was the Cyber-Watch Centre (CWC) implemented by the Infocomm Development Authority of Singapore (IDA) in 2007. Established using the Design-Build-Operate (DBO) model, the centre monitors cyber threats to government networks and acts as an early warning system for possible cyber attacks. The CWC has been successful, demonstrating the value of harnessing the expertise of the private sector to deliver a more effective and efficient cybersecurity service.

Not all cybersecurity PPPs in Singapore are standalone partnerships. Cybersecurity requirements are often included in other PPP arrangements. According to discussions with representatives in the energy sector, certain infrastructure projects funded by the Singapore government often build in CII protection requirements as part of the overall project cost.

While this is not intended to be a comprehensive examination of all PPP projects across the sectors, information available in the public domain allows us to briefly examine some of the key PPPs established in Singapore over the last few years (Table 2).

Table 2. Key Cybersecurity PPPs (2015-2016)

Area(s) of Focus	Name	Description
Multiple	Memorandum of Understanding (MOU) with various cybersecurity organisations	Over the last two years, Singapore's CSA has announced partnerships with Singtel, Check Point Software Technologies, FireEye, BAE Systems, $(ISC)^2$, Microsoft, Palo Alto Networks and CREST International to jointly work on various workforce development, research and development, and information sharing initiatives.
Workforce development	Singtel Cyber Security Institute (CSI)	Launched in April 2016 by Singtel in partnership with FireEye, Symantec and Palo Alto Networks with support from the Economic Development Board (EDB).
	Cyber Security Centre of Excellence	Launched in May 2016 by StarHub in partnership with Blue Coat, Cyberbit, EY, Fortinet and Wedge Networks with support from the EDB.
Research and development	Cyber Risk Management (CyRiM) Project	Launched in May 2016 by Singapore's Nanyang Technological University (NTU) and five insurance industry partners (Aon, Lloyd's, MSIG Insurance, SCOR and TransRe) with support from the Monetary Authority of Singapore (MAS) and CSA.

	ST Electronics-SUTD Cyber Security Laboratory	Launched in May 2016 by ST Electronics and the Singapore University of Technology and Design (SUTD) with support from NRF.
	NUS-Singtel Cyber Security Lab	Launched in October 2016 by the National University of Singapore (NUS) and Singtel with support from NRF.

In general, cybersecurity PPPs in Singapore tend to focus on three areas: workforce development, research and development, and information sharing. Mapping the above PPPs against Singapore's Cyber Security Strategy, we find that most of the PPPs fit under the "Developing a Vibrant Cybersecurity Ecosystem" pillar, which is focused on workforce development and research and development.

The main private sector parties in these PPPs generally come from Institutes of Higher Learning (IHLs), Research Institutes (RIs) and cybersecurity solution vendors (including cyber insurance). Although there are mutual benefits for the parties involved in these PPPs, it is not clear if they possess truly shared goals, although one can assume that the PPPs do allow the private-sector participants to further their commercial interests while achieving the goals of the public sector. This is often achieved through Key Performance Indicators (KPIs) that are commonly set in such arrangements. These may either be specific and concrete, or support a broader intent and purpose.

While some of the arrangements are supported by government grants or contracts, most of the cybersecurity PPPs in Singapore are established under some form of Memorandum of Understanding (MOU), which enables parties to start exploring the specifics of collaboration. Typically, an MOU in its initial stages may not specify tangible outcomes, resource commitments, or incentives for involved parties to act in a substantive manner to meet the goal. Only when the collaboration works out will the MOU then progress subsequently into an agreement or contract that defines more specific KPIs, as well as the human and financial resource commitments required.

What is notable about cybersecurity PPPs is that they are markedly different from the conventional approach taken in PPPs involving the government's procurement of services from the private sector on behalf of the public, as specified under the Ministry of Finance guidelines. These are the main differences:

- Cybersecurity PPPs tend to be based on a cooperative model that makes clear the intent of both parties, as opposed procurement PPPs based on the DBFO model.
- MOUs for cybersecurity PPPs are usually not legally binding or enforceable.
- Agreements are generally fixed, short term (less than 5 years) and limited to the funding period, hence relationships may not be for the long term (more than 25 years).

PPPs that fit under the "Building a Resilient Infrastructure" pillar of the Cyber Security Strategy are notably absent, even though this category would perhaps be most relevant to CII. This suggests that cybersecurity PPPs in Singapore tend to involve a more top-down approach, in which the government introduces a holistic CII Protection Programme (CIIPP) for owners and operators, building on the areas of improvement identified in the Cybersecurity Readiness Maturity Assessment programme of 2012.

The CIIPP requires owners and operators to take ownership and provide management focus to implement effective CII protection plans.

Private-sector CII owners and operators or end-user companies seem to have limited involvement in the above PPPs. While these companies are sometimes involved in proof-of-concept implementations or R&D projects, benefit directly from workforce development initiatives, and do have a shared goal with the other parties in the PPP, arguments can be made for them to have a stronger committed participation as a key stakeholder in the overall CII protection framework.

A look at the future of cybersecurity PPPs, and the potential impact of the new Cybersecurity Act being proposed, offers ideas on how such PPPs can be improved.

Future of Cybersecurity PPPs: How They Can Be Improved

In Singapore, highly-privatised sectors such as financial services are directed by relatively stringent cybersecurity-related regulations that are stronger than those in other sectors, which are still predominantly owned by the public sector and are therefore under a higher level of governmental control. Such an approach assumes that the private sector will respond adequately to government plans and implement recommended best practices. It should be noted, however, that stringent regulations and best practices still provide some leeway in implementation: the private sector may comply, but not necessarily in a manner that achieves the government's objectives. This can affect the effectiveness of the cybersecurity measures.

On the other hand, it can be argued that this regulatory approach has so far been effective because the government's demands have remained within the bounds of the private sector's business model and cost benefit analysis, and companies have therefore kept to them willingly. It remains to be seen whether this balance will continue to hold when the Cybersecurity Act comes up in 2018.

While public and private sector stakeholders are still working out the details of the Cybersecurity Act, the Cyber Security Strategy gives us a glimpse of how the new Act is likely to put in place a comprehensive framework to prevent and manage cyber incidents. Among other things, it will:

"*Require CII owners and operators to **take responsibility** for securing their systems and networks. This includes **complying** with policies and standards, **conducting** audits and risk assessments, and **reporting** cybersecurity incidents.*"

It is noteworthy that the framework requires CII owners and operators to "take responsibility", which implies that the government may hold them accountable for cybersecurity beyond their business interests. This would contrast the commonly-held view that the state should remain accountable for cybersecurity, and remain responsible for protecting critical infrastructure against significant threats such as organised crime, terrorists and threats from other states.

If the new Cybersecurity Act takes such an approach, it would signify a policy shift towards greater regulation and less reliance on market forces to ensure cybersecurity. While some of these requirements to comply with policies and standards may already be in place to some extent at the sectoral level, putting in place an industry-wide legislation

that cuts across all CI sectors will signal that the private sector has not responded adequately and that greater government control, enforcement and associated penalties are needed.

Another requirement being proposed is for CII owners and operators to facilitate the sharing of cybersecurity information with Singapore's CSA. Information sharing is a fundamental element in cybersecurity PPPs in most developed nations. Requiring it by law would signal that Singapore's current partnership model, which is based on voluntary participation and a grassroots approach, may be ineffective.

In the United States, debates have taken place on the usefulness of information sharing in its current form, and several observations have emerged:

- Security issues and strict required clearances can limit the sharing of information by the public sector with private sector individuals.[4] This can make the shared information generic and not actionable, reducing the value of partnerships.[9]
- Stringent review processes in the public sector can delay the release of time-critical information.[4]
- Information sharing may not take place in a meaningful way, resulting in recipients of shared information feeling dissatisfied with the quality of the information received, and parties becoming reluctant to share sensitive information of their own.

In Singapore, information sharing is facilitated by Security Operations Centres (SOCs) set up at the sectoral level. These centres facilitate the mandated collection of data and the monitoring and analysis of cyber threats. They may also act as an early warning system for impending attacks. According to information made available in the public domain, the Ministry of Home Affairs and the Land Transport Authority have established SOCs for their respective sectors, and the CSA hopes to set up similar centres in every sector.[17]

In addition, it is mandatory for CI owners and operators in certain sectors to report cybersecurity incidents to the regulator. Depending on the nature of the incident, these may then be reported to CSA. Besides allowing the regulator and CSA to determine if the incident is of a systemic nature, this also creates another means of information sharing, as threat information may be useful for other CI sectors.

Conversations with sector representatives indicate that the private sector generally trusts the Singapore government as a clearing house for such information, though the information flow may not be balanced. Some have observed that while the private sector reports detailed information on incidents and sends detailed threat data to the SOCs, the indicative analysis coming back from the public sector tends to lack actionable details and context. Understandably, there is always a challenge in determining how much information can and should be shared. If the information is sensitive, sharing it may prove detrimental to companies within and across sectors, affect buying decisions, or affect a company's strategic positioning of its product and services. As the information sharing model matures, different parties will have to work out an equitable model that provides mutual benefits while still working towards a shared goal.

[17] Loke, Kok Fai. "Cyber Security Agency Looking to Strengthen Online Security in Every Sector - Channel NewsAsia." Channel NewsAsia, January 1, 2016. http://www.channelnewsasia.com/news/singapore/cyber-security-agency/2392484.html.

Other nations have taken a more grassroots approach to information sharing. The United States Department of Defense's Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) and Japan's Initiative for Cyber Security Information Sharing Partnership (J-CSIP), both created in 2011, allow for mutual sharing of cyber threat information between defence industries and government. Non-disclosure agreements are made, and the use and sharing of information are both kept voluntary as a way of incentivising companies to join while not pressuring them to commit. This bottom-up operational structure was devised following the failure of past partnerships that were rigid and based on legally-binding contracts, which discouraged teamwork and efficiency. Those tie-ups had also featured strict constraints enforced from a distant command structure, which also meant that the PPPs were less able to respond flexibly to the fluid nature of cyber attacks.[18]

In a nation with a strong regulatory stance like Singapore, many CI owners and operators are concerned that sharing sensitive information with regulators will "come back and bite you" in the future. This is because the sector authorities, while acting as clearing houses for shared cybersecurity data and incidents, also act as regulators, and possess the supervisory powers to issue licences and impose penalties. Mechanisms must therefore be set up to assure CI owners and operators that they can share information without suffering regulatory repercussions. As an example, the Monetary Authority of Singapore (MAS) has set an example by including a concession that such information cannot be used by the Financial Supervision Group.

Singapore's top-down, mandatory approach presumably allows its government to get a sector-level view of the cyber threat environment. While the extent and depth of data collection and analysis is not clear, this participation model may alleviate concerns among private CII owners and operators that they will be held responsible for national security, and assure them that the government remains fully responsible for monitoring cyber threats at both the sector and national level.

On the surface, Singapore's efforts in information sharing are worthwhile and suggest a desire to foster partnerships within Singapore and internationally. There is, however, a crucial need to institute adequate measures of success. Otherwise, such partnerships may give the false impression that the mere sharing of information, regardless of quality and robustness, will create a more cyber secure environment, and encourage private CII owners and operators to believe that they have done their part simply by providing minimal data pertaining to their own cyber insecurities.[9]

A successful PPP is built on shared goals, mutual trust, clear strategies, appropriate distribution of risks, well-defined responsibilities and authority, and clearly defined rules.[8] [4] [19] More importantly, given the substantial financial investments involved, a successful PPP has as its cornerstone economic viability and a "sound financial package". In situations where one party places greater priority on a shared goal and has

[18] Manley, Max. "Cyberspace's Dynamic Duo: Forging a Cybersecurity Public-Private Partnership Cyberspace' S Dynamic Duo: Forging a Cybersecurity Public-Private Partnership." Journal of Strategic Security 8, no. 5 (2015): 85–98. doi:10.5038/1944-0472.8.3S.1478.

[19] Zhang, Xueqing. "Critical Success Factors for Public–Private Partnerships in Infrastructure Development." Journal of Construction Engineering and Management 131, no. 1 (January 2005): 3–14. doi:10.1061/(ASCE)0733-9364(2005)131:1(3).

a higher dependency on the other party, especially, there must be some forms of incentives or financial arrangements to make the partnership attractive to both parties.

An examination of Singapore's cybersecurity strategies, plans and multi-pronged approach of legislation, regulation and PPPs suggests that there exist opportunities to enhance the public sector's engagement with the private sector in several ways:

- Cybersecurity PPP report cards: Given the substantial use of public funds, having the government's Auditor-General conduct a closer examination of cybersecurity PPPs may help ensure that substantial value is created through such public-private sector arrangements. This would also require well-defined standards of measurement that are specific to the workings of PPPs.
- Enhance PPPs with private sector CII owners: The government currently uses regulation as the main tool for raising cybersecurity levels for CII, while PPPs appear to be limited to information-sharing arrangements that are mostly mandated rather than voluntary. There may be opportunities for greater committed participation by private sector CIIs in workforce development and R&D PPPs.
- Use PPPs to upgrade cybersecurity: Given today's complex business relationships and interconnected technologies, security is only as strong as the weakest link. The overall cybersecurity of CI sectors is therefore dependent on the maturity level of other related sectors. PPPs could thus be used to upgrade cybersecurity to higher levels. These arrangements may include co-funding for cybersecurity implementations, insurance, and legal protection or "safe harbour" provisions for compliance.

There is a stronger imperative now, more than ever, for greater partnership between the public and private sectors to secure cyberspace especially in the critical infrastructure sectors. While these partnerships may on the surface project a positive approach to improve cybersecurity standards, we need a mindset of growth to keep monitoring the effectiveness of PPPs and enhance the mechanisms of these arrangements so that they can deliver greater value as a public service.