Ponder the Improbable since 1996

SUCCESSFUL CYBER-RISK MANAGEMENT OF OPERATIONAL TECHNOLOGY AND INDUSTRIAL CONTROL SYSTEMS – TECHNICAL AND POLICY RECOMMENDATIONS

Adam Palmer
Michael Rothschild
Benjamin Ang

Policy Report
February 2021

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Policy Report

SUCCESSFUL CYBER-RISK MANAGEMENT OF OPERATIONAL TECHNOLOGY AND INDUSTRIAL CONTROL SYSTEMS – TECHNICAL AND POLICY RECOMMENDATIONS

Adam Palmer
Michael Rothschild
Benjamin Ang

February 2021

TABLE OF CONTENTS

Executive Summary

Cyberattacks are on the rise against Operational Technology (OT) systems. These are the interconnected devices and controllers commonly deployed in sectors such as manufacturing, transportation, energy, and water management. Advances in IT networks have led to a convergence of risk between OT and IT (Information Technology) systems. This paper examines the challenges and best practices in responding to this convergence and discusses some of the technical measures that can be used to improve the security of OT devices. The paper includes a focus on Singapore's OT risk management approach outlined in the Singapore OT Cybersecurity Masterplan. The paper also includes comments on the OT challenges facing the Asia-Pacific region, and suggests how Singapore, in private-public partnership with industry groups, can improve the capacity for OT security in the Asia-Pacific region.

Overview of the OT Security Challenge

Many organisations lack basic visibility of their IT and OT infrastructures, and do not take basic cyber-exposure countermeasures. This allows a multitude of cyberthreat actors to easily exploit vulnerabilities undetected. In one survey, one-third of IT professionals in Europe reported that their organisations had been breached as a result of known vulnerabilities.[1] Advanced attacks only caused about 1–2 per cent of major breaches.

Today's advanced "Smart" (i.e., connected) OT environment has enlarged the extent of cyberattacks. Cyberthreat actors can enter through weak links in the IT environment, and through "lateral movements", quickly penetrate the OT environment or vice versa across the entire network. This has been highlighted in recent cyberattacks against OT devices on networks, like the data breach of Target retail stores in 2013 through its heating, ventilation and air-conditioning (HVAC) system,[2] and more recently the "Lemon Duck" malware in 2019 targeting connected devices, including access controls of heavy equipment. Credible threats of cyberattacks have also been made against sensitive operations, like nuclear power plants. There was a 200 per cent increase in the number of organisations that reported between 6–10 incidents between 2017–2019.[3]

OT-related risks are expected to increase as more industrial operations combine complex IT and OT infrastructures with thousands of devices connected via the Industrial Internet of Things (IIoT), as more organisations use smart HVAC and lighting controls to manage buildings and workspaces more efficiently, and more cities strive to become smart cities.

Most cyberattacks thus far were centred on Industrial Control Systems (ICSs). Depending on the type of industry, this may be referred to as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs) or Distributed Control System (DCSs). These controllers are extremely reliable and may control anything from cooling stations and turbines to electrical grids, and oil and gas refineries. Because of their reliability, many of these devices have been left unchanged for years. When these ICSs were first deployed, they were not required to be connected to networks, so most were not designed to

---

1 Ranger, Steve. "Cybersecurity: One in three breaches are caused by unpatched vulnerabilities." 4 June 2020. https://www.zdnet.com/article/cybersecurity-one-in-three-breaches-are-caused-by-unpatched-vulnerabilities/

2 Krebs, Brian. "Target Hackers Broke in Via HVAC Company." February 2014. https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

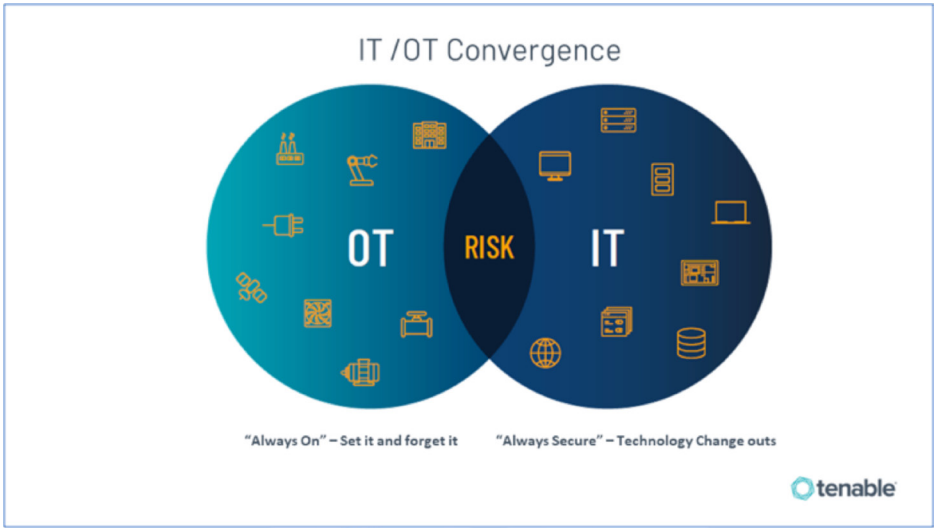
3 SANS 2019 State of OT/ICS Cybersecurity Survey, cited in Singapore's OT Cybersecurity Masterplan

address the cybersecurity threats or human errors of today, and especially not the new cyberattacks launched by well-funded and highly motivated criminals or even nation states. Advances in technology have exposed these devices online, and made them major targets for cyber-attackers. Risky activities by cyber-attackers, such as changes to devices made via direct connections, could remain undetected by passive network monitoring of traditional IT networks. If the organisation misses a cyberattack on an OT device, the device might remain infected for days, weeks or even months undetected.

The Convergence of IT and OT Risk

Few organisations currently manage OT and IT with the same level of staffing and resources. Both have traditionally operated in different "worlds" with different priorities. To address the new complex blended OT/IT threat, many industrial organisations have begun to converge their IT and OT groups. The "convergence initiative" is often challenging as it brings together two substantially different systems, requiring alignment of strategic goals, collaboration, and training.

Figure 1: IT/OT Risk Convergence



Source: Tenable

The biggest differences between IT and OT environments are in their pedigree, approach, background, and mindset. IT staff are typically concerned about data confidentiality, integrity, and availability, and operate in a dynamic environment where systems are constantly upgraded and replaced. OT staff work are typically concerned about stability, safety, and reliability of the complex and sensitive environment, typically built on legacy systems that have existed for decades, with the mindset that “if it works, don’t touch it”. OT engineers often recoil at the thought of IT personnel being involved in the safety of their industrial facilities or tinkering with their ICSs. These ICSs often use proprietary network protocols, and lack basic security controls, like authentication, encryption, event logs or audit trails.

Technical Challenges for OT Security

Traditional passive network monitoring is not sufficient to detect all OT risks as it does not detect threats that may lie dormant or communicate across the network. Active querying of assets in the OT environment, including device-based security, provides a better situational analysis for the OT environment. Actively querying devices in the OT network to validate their status provides a granular level of asset risk awareness. This enhances the ability to automatically discover and classify all ICS assets from Windows machines to lower-level devices like PLCs, RTUs, and DCS, even when they are not communicating across the network. Active querying can also identify local changes in device meta-data, e.g., firmware version, configuration details and state, as well as changes in the code/function blocks of device logic. Active querying technology should use read-only queries in native controller communication protocols to be completely safe from any negative impacts on queried devices. Since active querying eliminates the need to monitor every switch in the organisation, it can also save some maintenance costs.

OT systems usually do not share inventory information across the network, although maintaining a granular and up-to-date asset inventory is key to controlling this OT environment. Active querying of devices can ensure the asset inventory is complete and accurate, and even discover dormant industrial devices that are connected to the network but not communicating.

Employees, contractors and system integrators who are connected to control devices with a serial cable or USB device would also pose a risk. A malicious actor with physical access to the network can connect to controllers directly, or an employee or contractor could unknowingly expose controllers to infection by connecting to an infected laptop or USB drive. Organisations need

to periodically capture device snapshots to identify if configuration changes have occurred and validate that no one has compromised OT device integrity.

All the technical information is meaningless without contextual information. When organisations have detected suspicious network events, they would need technologies such as active querying of relevant devices to gather contextual details.

Standards and Compliance in Singapore's OT Cybersecurity Masterplan

While OT security requires allocation of resources to improve security, organisations might be reluctant to do this due to costs or resource concerns. Some countries have used security standards and regulatory compliance to drive business priorities towards addressing the converging OT/IT cyber-risks.

Two of the earliest standards for OT security were the 2008 North American Electricity Reliability Corporation (NERC) and the US Federal Energy Regulatory Commission (FERC) requirements. These regulations apply to IT and OT oversight in critical infrastructures that require the staff to collaborate and share relevant risk data to ensure security and reliability. They specifically call for an environment that has the ability to conduct forensics across both IT and OT networks in order to identify, mitigate, and report on incidents that could disable industrial operations and critical infrastructure.[4]

The Cyber Security Agency of Singapore (CSA) published Singapore's Operational Technology (OT) Cybersecurity Masterplan[5] in October 2019 to enhance the security and resilience of Critical Information Infrastructure (CII) sectors that deliver essential services across Singapore. This focus on CII builds on the first of four pillars of Singapore's Cyber Security Strategy[6] published in 2016. Singapore is particularly concerned about OT security because of its Smart Nation initiative[7], where the hyper-connected economy is powered by digital innovation in the key domains of health, transport, urban

[4] Rothschild, Michael. "Mind the Gap: How to Align Your IT and Operational Technology Teams." 3 July 2018. https://www.tenable.com/blog/mind-the-gap-how-to-align-your-it-and-operational-technology-teams

[5] CSA. "Singapore's Operational Technology Cybersecurity Masterplan 2019." 1 October 2019. https://www.csa.gov.sg/news/publications/ot-cybersecurity-masterplan

[6] CSA. "Singapore's Cyber Security Strategy." 10 October 2016. https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy

[7] Smart Nation Singapore. "Transforming Singapore Through Technology." 18 November 2018. https://www.smartnation.gov.sg/why-Smart-Nation/transforming-singapore

solutions, finance, and education — all of which have underlying OT systems that need to be protected.

Although the Masterplan is primarily aimed at CII owners who operate OT systems, it can apply to other enterprises running OT systems, including manufacturing plants in the oil and gas sector, and semiconductor factories. Key thrusts under the Masterplan include:

1. **Providing OT cybersecurity training** for the CII sectors, through the CSA Academy and training partners, to equip professionals with skills, including OT cybersecurity ethical hacking knowledge, to handle cyberattacks on ICS facilities.

2. **Sharing of cybersecurity information through the OT Information Sharing and Analysis Center (OT-ISAC)**. CSA together with Global Resilience Federation Asia Pacific (GRF APAC) launched OT-ISAC in 2019, with members from government agencies, and CII and OT industries. CSA provides guidance and the initial funding while GRF APAC manages the centre. Cyberthreat sharing is community driven. OT-ISAC's activities include the OT-ISAC Virtual Summit 2020[8] for chief information security officers (CISOs) and OT/IT experts across Asia.

3. **Publishing the OT Cybersecurity Code of Practice (CCoP)** to strengthen OT owners' policies and processes. The Cybersecurity Code of Practice for Critical Information Infrastructure[9] incorporated in January 2020 refers to international standards for OT cybersecurity such as IEC 62443-3 (Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels).

4. **Adopting technologies for cyber-resilience through public-private partnerships** via the National Cybersecurity Research and Development Programme, which has funding support of over S$190 million (US$138 million), industry calls for innovation, and sectoral Security Operations Centres. Projects developed so far include software to take inventory of OT assets and identify unauthorised OT devices for the water sector; a SCADA packet inspection firewall and secure wireless communications for the land transport sector; and prototypes to detect anomalous activities of OT systems for the energy sector.

---

[8] OT-ISAC. "Virtual Summit 2020." Accessed 24 November 2020. https://www.otisac.org/ot-isac-summit-2020

[9] CSA. "Codes of Practice / Standards of Performance." Accessed 24 November 2020. https://www.csa.gov.sg/legislation/codes-of-practice

5. **Encouraging security by design** in OT equipment manufacturers and service providers where cybersecurity measures are designed into devices at the developmental phase.

Under the Masterplan, Singapore has established an Operational Technology Cybersecurity Expert Panel (OTCEP) in 2020 that comprises local and international OT cybersecurity experts. OTCEP discusses key global OT technologies and emerging trends, and recommends best practices to the government to address cybersecurity challenges and gaps.[10]

In a related move in 2020, Singapore launched a Cybersecurity Labelling Scheme (CLS) for consumer smart devices to improve Internet of Things (IoT) security. The first in Asia Pacific, CLS has begun labelling for Wi-Fi routers and smart home hubs[11]. A similar scheme could also be created for IIOT devices to develop a holistic approach to OT security.

Best Practices for OT Security Implementation

Singapore's OT Cybersecurity Masterplan accurately identifies that OT cybersecurity involves not only technical issues, but people and processes. Policy measures must therefore include openness and interoperability, and the Masterplan calls for a platform of trust and communication to facilitate information sharing among sectors and businesses.

Within an organisation, an effective OT/IT security programme should be both risk-based and prioritised, focusing on vulnerabilities that are at high risk of being exploited. Risk-based prioritisation saves time and resources to focus on critical areas. This requires organisations to understand where they are exposed by using some of the technical measures described earlier. Security leaders can then drill down into specific vulnerabilities and identify controls that are most effective at reducing the risks. A mature and effective Vulnerability Management Programme should be used to view, validate, and prioritise vulnerabilities, while understanding the context of these risks.

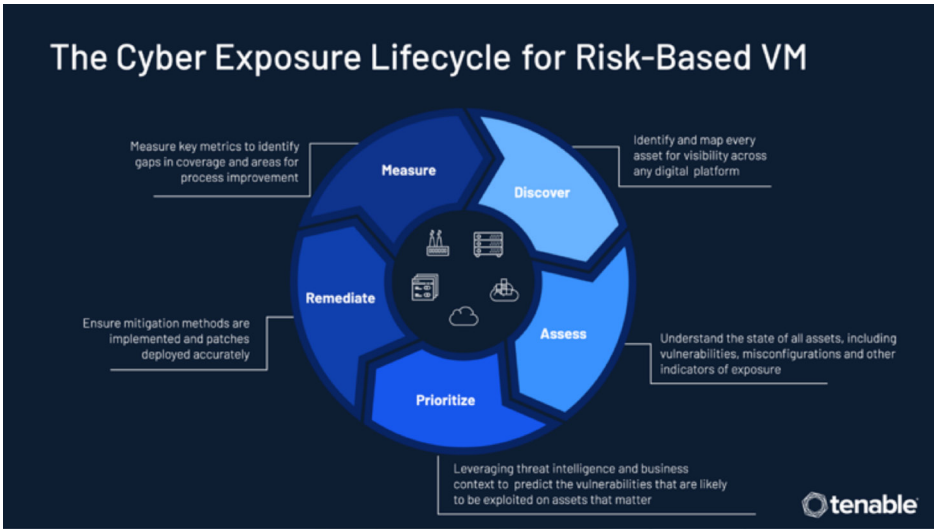
[10] CSA. "Singapore International Cyber Week 2020 - Highlights and Testimonials." Press Release, 19 October 2020. https://www.csa.gov.sg/news/press-releases/sicw-2020-highlights-and-testimonials

[11] Baharudin, Hariz. "New cyber security label for smart home devices launched; plans to have standards adopted overseas." *The Straits Times*, 7 October 2020. https://www.straitstimes.com/singapore/new-cyber-security-label-for-smart-devices-launched-plans-to-have-standards-adopted

A 2019 study by McKinsey Consulting found that risk-based vulnerability management reduces risk "by building the appropriate controls for the worst vulnerabilities, to defeat the most significant threats — those that target the business's most critical areas. [This] approach allows for both strategic and pragmatic activities to reduce cyber-risks. Companies have used the risk-based approach to increase their projected risk reduction 7.5 times above the original [security] programme at no added cost."[12]

With risk-based vulnerability management, the question isn't "How do we protect against and remediate all of these vulnerabilities?" but "Which vulnerabilities pose the greatest risk?" Effective vulnerability management can significantly reduce costs and man efforts, while delivering better cybersecurity.

Figure 2: Cyber-exposure Lifecycle for Risk-based VM



Source: Tenable

[12] Boehm, J., Merrath, P., Poppensieker, T., Riemenschnitter, R., and Stähle, T. "Cyber risk management and the holistic cybersecurity approach." *McKinsey on Risk*, Issue 6 - Winter 2019. Accessed 24 November 2020. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/McKinsey%20on%20Risk%20Issue%206%20Winter%202019/McKinsey-on-Risk-Issue-6-Winter-2019.pdf

OT Security Across the Asia-Pacific Region

Asia Pacific is predicted to become the leading region[13] in terms of 5G technology adoption with some 1.14 billion potential subscribers that would account for 65% of global 5G subscriptions by 2024. The leading 5G countries will likely be South Korea, China, Japan, and Australia. ASEAN also launched the ASEAN Smart Cities Network (ASCN) in 2018, a collaborative platform where the ten ASEAN member states move towards the common goal of smart and sustainable urban development[14] using digital technology such as IoT. While adoption of 5G will enable wider implementation of IoT and robotics in OT, it will also broaden the cyberattack surface.

Critical infrastructure and OT in Asia have already experienced multiple cyberattacks[15]. South Korea has accused North Korea of preparing a cyberattack on its railway control system in March 2016. An Iranian cyber-espionage group allegedly targeted a South Korean petrochemical company in September 2017. India's tallest hydroelectric and water supply dam was attacked by malware in 2017. A major cyber-sabotage group was revealed to be targeting electric utilities in Asia in February 2019.

There are numerous challenges that countries in Asia Pacific will need to address, starting with the disparity of cyber-maturity and enforcement of cybersecurity requirements. The cybersecurity skills and knowledge levels of OT operators and regulators in ASEAN member states vary greatly. Only a few ASEAN member states have issued legislation, regulations, and guidelines to address OT cybersecurity.

Policy Recommendations

Because of differing levels of maturity for OT security policy across the Asia-Pacific region, there is a need for industry groups to take a lead in developing and harmonising best practices in cybersecurity. The guidance can support policy development in individual countries to address specific national or

[13] Global Data. "Asia-Pacific will lead 5G technology adoption by 2024, says GlobalData." 13 January 2020. https://www.globaldata.com/asia-pacific-will-lead-5g-technology-adoption-2024-says-globaldata/

[14] ASEAN Smart Cities Network. https://asean.org/asean/asean-smart-cities-network/

[15] Lin, M., and Janot, E. "Building cybersecurity into infrastructure." Accessed 24 November 2020. https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sg-risk-building-cyber-security.pdf

industrial needs. Industry groups like GRF APAC and OT-ISAC have already been working closely with governments in Asia Pacific. They can take the lead in developing harmonised regional OT standards, especially in cooperation with Singapore which the United Nations (UN) considers to be a "global leader in the field of cybersecurity" and actively contributing internationally.[16]

In addition to regional harmonisation, there must also be alignment with international, consensus-driven standards. For example, ASEAN member states can begin to take guidance from the ASEAN Ministerial Conference on Cybersecurity (AMCC), which agreed in 2018[17] to subscribe in-principle to the 11 voluntary, non-binding norms recommended in the 2015 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE), as well as to focus on regional capacity building in implementing these norms. These norms include Critical Infrastructure Protection, and therefore OT protection. Singapore and the UN agreed in 2020 to develop a checklist with steps for countries to implement these 11 norms. This process, built on a system developed by ASEAN, will be facilitated through workshops carried out through the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) under the auspices of the UN-Singapore Cyber Programme (UNSCP).[18]

ASCCE is one of the entities providing regional capacity building in Asia Pacific[19]. It provides programmes for ASEAN senior policy and technical officials with decision-making responsibilities, together with ASEAN member states, ASEAN dialogue partners, and other international partners including Australia, Canada, the European Union, Japan, New Zealand, Republic of Korea, United Kingdom, and United States. ASCCE has focused on international law, cyber strategy, legislation, cyber norms, and other cybersecurity policy issues; provided CERT-related technical training; facilitated the exchange of open-source cyber-threat and cyberattack-related information and best practices; and conducted virtual cyber-defence trainings and exercises. ASCCE would be a good platform to provide capacity-building programmes for ASEAN member states' OT regulators and operators, drawing on resources from Singapore's OT Cybersecurity Masterplan and OTCEP.

---

[16] Ibid.

[17] CSA. "ASEAN Member States Agree to Strengthen Cyber Coordination and Capacity-Building Efforts." Press Release, 19 September 2018. https://www.csa.gov.sg/news/press-releases/amcc-2018

[18] "Singapore to work with UN to help nations implement norms for responsible cyber behaviour." *The Straits Times*, 2 November 2020. https://www.straitstimes.com/tech/singapore-to-work-with-un-to-help-nations-implement-norms-for-responsible-cyber-behaviour

[19] CSA. "ASEAN Singapore Cybersecurity Centre of Excellence." Fact Sheet, 2 October 2019. https://www.csa.gov.sg/-/media/csa/documents/sicw_2019/amcc/factsheet-ascce-2019.pdf

The future of growth and technology development in the Asia-Pacific region requires cooperation and recognition that the traditional IT threat landscape has expanded. The threat landscape now includes personal mobile devices used for work, cloud technology, IoT technologies, and connected OT devices. OT is critical not just for heavy industries, but today's highly connected smart cities. The public and private sector must work cooperatively to create a future that supports both growth and security for OT.

About the Authors

Adam Palmer leads Tenable engagement with CISO on cybersecurity strategy. He has more than 20 years of cybersecurity leadership experience including roles at Banco Santander, FireEye, Symantec, and the Bank Policy Institute. He served as a founding member of the United Nations Global Programme Against Cybercrime.

Michael Rothschild is the Senior Director of Marketing who comes to Tenable by way of the Indegy acquisition. He focuses on the OT product line. Michael is an advisory board member at Rutgers University and is a past professor of marketing. Michael has a number of published works in marketing and healthcare. In his spare time, he is a first aid instructor and volunteers as an EMT.

Benjamin Ang is a Senior Fellow and Deputy Head in the Centre of Excellence for National Security (CENS) at RSIS. He leads the Cyber and Homeland Defence Programme of CENS, which explores policy issues around the cyber domain, international cyber norms, cyberthreats and conflict, strategic communications and disinformation, law enforcement technology and cybercrime, smart city cyber issues, and national security issues in disruptive technology.

Prior to this, he had a multi-faceted career that included time as a litigation lawyer arguing commercial cases, IT Director and General Manager of a major Singapore law firm, corporate lawyer specialising in technology law and intellectual property issues, in house legal counsel in an international software company, Director-Asia in a regional technology consulting firm, in-house legal counsel in a transmedia company, and senior law lecturer at a local Polytechnic, specialising in data privacy, digital forensics, and computer misuse and cybersecurity.

Benjamin graduated from Law School at the National University of Singapore and has an MBA and MS-MIS (Masters of Science in Management Information Systems) from Boston University. He is qualified as an Advocate and Solicitor of the Supreme Court of Singapore, and was a Certified Novell Network Administrator back in the day. He also serves on the Executive Committee of the Internet Society Singapore Chapter.

About the Centre of Excellence for National Security

The **Centre of Excellence for National Security (CENS)** is a research unit of the S. Rajaratnam School of International Studies (RSIS) at the Nanyang Technological University, Singapore.

Established on 1 April 2006, CENS raison d'être is to raise the intellectual capital invested in strategising national security. To do so, CENS is devoted to rigorous policy-relevant analysis across a range of national security issues. CENS is multinational in composition, comprising both Singaporeans and foreign analysts who are specialists in various aspects of national and homeland security affairs. Besides the work undertaken by its full-time analysts, CENS boosts its research capacity and keeps abreast of cutting edge global trends in national security research by maintaining and encouraging a steady stream of Visiting Fellows.

For more information about CENS, please visit www.rsis.edu.sg/cens.

About the S. Rajaratnam School of International Studies

The **S. Rajaratnam School of International Studies (RSIS)** is a think tank and professional graduate school of international affairs at the Nanyang Technological University, Singapore. An autonomous school, RSIS' mission is to be a leading research and graduate teaching institution in strategic and international affairs in the Asia Pacific. With the core functions of research, graduate education and networking, it produces research on Asia Pacific Security, Multilateralism and Regionalism, Conflict Studies, Non-traditional Security, Cybersecurity, Maritime Security and Terrorism Studies.

For more details, please visit www.rsis.edu.sg. Join us at our social media channels at www.rsis.edu.sg/rsis-social-media-channels or scan the QR code.

RSiS | S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

Nanyang Technological University, Singapore

Nanyang Technological University, Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg