ERIA Research Project Report FY2025, No. 39

Promoting Cyber Security for Distributed Energy Systems (DES) and Smart Grids in ASEAN

Edited By

ERIA Asia Zero Emission Center (AZEC)

Nomura Research Institute Singapore Pte. Ltd.

Economic Research Institute for ASEAN and East Asia

Promoting Cyber Security for Distributed Energy Systems (DES) and Smart Grids in ASEAN

Economic Research Institute for ASEAN and East Asia (ERIA)

Sentral Senayan II 6th Floor

Jalan Asia Afrika No. 8, Gelora Bung Karno

Senayan, Jakarta Pusat 12710

Indonesia

ERIA Research Project Report FY2025 No.39

Published in January 2026.

Foreword

The ASEAN region stands at a pivotal juncture in its energy transition. As member states accelerate their shift toward cleaner and more decentralised energy systems, the integration of distributed energy resources such as solar, wind, and battery storage is transforming the energy landscape. This transition brings with it the promise of a more sustainable and resilient future but also introduces a new and urgent challenge: cybersecurity.

Distributed energy systems (DES) rely heavily on digital technologies for monitoring, control, and integration into national grids. With this digitalisation comes increased exposure to cyber threats that could compromise energy security, disrupt critical infrastructure, and hinder progress toward climate goals. In light of this, ensuring the cybersecurity of DES is no longer optional – it is essential.

Drawing from global best practices, this study provides timely and critical insights and develop basic concept to strengthen the cybersecurity framework for DES across the ASEAN region, promoting both energy security and sustainability. It aligns with the broader vision of the Asian Zero Emission Community (AZEC), aiming not only to safeguard ASEAN's energy future but also to foster a collaborative approach to regional energy resilience.

The insights gleaned from this study will serve as a critical resource for ASEAN countries as they strive to achieve their energy transition goals while maintaining robust cybersecurity. This report marks an important milestone in our efforts to build a secure, sustainable, and inclusive energy ecosystem in ASEAN. We look forward to continuing this collaboration and ensuring that the basic concept developed through this project are successfully disseminated and implemented across the region.

Naoto Okura
Director General for Research and Policy Design, ERIA

Preface

Asia's rapid economic growth has been accompanied by a substantial increase in energy demand and associated carbon emissions. The rising global average temperature, driven by growing energy use, underscores the necessity for rapid decarbonisation. However, this must be balanced with the assurance of continued economic growth, especially in regions such as ASEAN, where energy demand is expected to continue growing due to economic development. Achieving this balance requires innovative solutions, and distributed energy systems (DES) and microgrids powered by renewable energy sources offer promising pathways. These systems enable decentralised energy generation, which is crucial for enhancing grid resilience, especially in remote areas, while contributing to carbon neutrality.

The potential of smart grids, particularly those utilising renewable energy such as solar, wind, and biomass, cannot be overstated. These distributed energy resources (DERs) provide flexibility, reduce transmission losses, and can help mitigate the volatility of energy supply. Nevertheless, as energy grids become more decentralised, the accompanying risk of cyberattacks increases. These cyber-threats pose significant risks to the stability of energy supply, particularly in systems that rely on smart technologies for real-time control and monitoring.

This research project seeks to address the dual challenge of promoting the use of distributed energy resources while enhancing the cybersecurity of distributed energy systems. As part of the broader vision to realise the Asian Zero Emission Community (AZEC), this project aims to support ASEAN countries in their energy transition by promoting renewable energy adoption and developing action plans that include a basic concept for cybersecurity for DES. The collaboration between ASEAN nations is critical to ensuring that the region not only advances toward its decarbonisation goals but does so securely, safeguarding critical infrastructure from potential cyber threats.

The authors hope that this report will contribute to ongoing efforts within ASEAN to promote energy security and sustainability. By providing a roadmap for the safe and widespread adoption of DES and establishing a shared basic concept for their cybersecurity, it is our aspiration that these insights will support policymakers, industry leaders, and stakeholders in building a more resilient and sustainable future for the region.

Hiroshige Muraoka
President of Nomura Research Institute Singapore Pte. Ltd.

Acknowledgements

This study was undertaken based on close collaboration with our partners in ASEAN, industry specialists, academic researchers, and government officials who are focused on the expansion of distributed energy resources as well as related cybersecurity initiatives to improve energy security in Southeast Asia. The authors particularly would like to thank all the participants in the various meetings, discussions, and study groups, as well as other participants who were involved in the project in one way or another.

The presentations at the study groups – held by the government authorities, industry players, academic researchers, and other stakeholders – and ensuing discussions will play a pivotal role in providing direction and inspiring relevant parties to develop future strategies and policy measures to support the expansion of distributed energy resources as well as related cybersecurity initiatives.

The authors would also like to express sincere appreciation to all experts involved, for their kind and generous support for this study, without which this report would not be possible. All errors and mistakes are the authors' responsibility.

Hiroshige Muraoka
President of Nomura Research Institute Singapore Pte. Ltd.

List of Project Members

Project Coordinator
Kei Sudo
Senior Policy Advisor, ERIA

Project Manager
Hiroshige Muraoka
President, NRI Singapore

Project Leader
Katsuya Tokuda
Manager, NRI Singapore

Members
Jacqueline Acacia Poernomo
Senior Consultant, NRI Singapore

Cameron Wang Jing
Senior Consultant, NRI Singapore

Nicholas Wong Wei Yong
Senior Consultant, NRI Singapore

Albert Jeremy P. Hutagaol
Consultant, NRI Singapore

External Experts
Masaki Umejima
Convener of the Smart Energy Development Plan, System Committee, International Electrotechnical Commission

Kaori Suzuki
Secretariat of Cyber Civilisation Research Center (CCRC), Keio University Global Research Institute (KGRI)

Contents

List of Figures

List of Tables

List of Abbreviations and/Acronyms

ACE	ASEAN Centre for Energy
ACSC	Australian Cyber Security Centre
ADB	Asian Development Bank
ADGSOM	ASEAN Digital Senior Officials Meeting
ASEAN	Association of Southeast Asian Nations
AZEC	Asian Zero Emission Community
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security, Germany)
CEDS	Cybersecurity for Energy Delivery Systems
CII	Critical Information Infrastructure
CIP	Critical Infrastructure Protection
CISC	Cyber and Infrastructure Security Centre
CIX	Climate Impact X
CPPA	Corporate Power Purchase Agreement
CPSF	Cyber Physical Security Framework
CSA	Cyber Security Agency of Singapore
DER	Distributed Energy Resources
DES	Distributed Energy Systems
DICT	Department of Information and Communications Technology (Philippines)
DOE	Department of Energy
DR	Demand Response
DSO	Distribution System Operator
ERAB	Energy Resource Aggregation Business
ERIA	Economic Research Institute for ASEAN and East Asia
ESEOC	Energy Sector Emergency Operations Centre
FERC	Federal Energy Regulatory Commission
IEC	International Electrotechnical Commission
IL	Interruptible Load
IPA	Information Technology Promotion Agency
JICA	Japan International Cooperation Agency
MES	Mobile Energy System

METI	Japan Ministry of Economy, Trade and Industry
NARUC	National Association of Regulatory Utility Commissioners
NCSC	National Cybersecurity Centre
NEMS	National Electricity Market of Singapore
NERC	North American Electric Reliability Corporation
NISC	National Centre of Incident Readiness and Strategy for Cybersecurity
NRI	Nomura Research Institute
NSP	National Security Policy
RES	Renewable Energy Sources
SGDSN	Secretariat-General for Defence and National Security (France)
SP	Singapore Power
TPC	Temporary Price Cap
TSO	Transmission System Operator
USEP	Uniform Singapore Energy Price
VPP	Virtual Power Plant
WESM	Wholesale Electricity Spot Market

Executive Summary

This study aims to address the critical need for enhanced cybersecurity in distributed energy systems (DES) and smart grids within the ASEAN region. As ASEAN Member States transition toward cleaner, renewable energy sources, the decentralisation of energy through distributed resources like solar, wind, and battery storage is becoming a key feature of modern energy infrastructure. However, this shift also introduces heightened cybersecurity risks that must be addressed to ensure stable and resilient energy supply.

The overarching goals of this study are to promote the adoption of secure DES in ASEAN, contribute to the realisation of the Asian Zero Emission Community (AZEC), and establish a Basic Concept of Cybersecurity for DES that can be widely disseminated across the region. The study also aims to develop a robust action plan to mitigate the risks associated with cyberattacks on energy infrastructure, which is crucial for ensuring both energy security and sustainability.

Key Findings

- Growth of Distributed Energy Systems: ASEAN nations are increasingly adopting DES technologies, particularly renewable energy microgrids, to support their decarbonisation efforts and meet rising energy demand. This trend is in line with global movements towards a cleaner, decentralised energy grid.
- Increased Cybersecurity Vulnerabilities: The growing reliance on digital technologies for managing energy systems has made DES more susceptible to cyberattacks. Countries with advanced DES deployments have already experienced notable incidents, highlighting the urgent need for enhanced cybersecurity measures.
- Varying Levels of Cybersecurity Preparedness in ASEAN: While some ASEAN countries have made strides in developing cybersecurity frameworks for critical infrastructure, others are still in the early stages of understanding and addressing the cyber risks associated with DES. There is a significant gap in regional cooperation and policy harmonisation on cybersecurity for DES.
- ERAB as the Next Step after DES: Following Japan's footsteps in the creation of an integrated grid network where energy aggregators play a central role through the development of DES deployment, countries in ASEAN can learn from Japan's best practices for future ERAB implementation as well as the creation of a basic concept of cybersecurity for ERAB.

Key Barriers and Issues

- Lack of Comprehensive Cybersecurity Frameworks: A major barrier to securing DES in ASEAN is the absence of comprehensive cybersecurity policies that specifically address the unique risks posed by distributed energy systems. Current frameworks tend to focus on traditional, centralised energy systems and are not fully equipped to handle the decentralised nature of DES.
- Fragmented Regional Coordination: There is a lack of unified regional guidelines or collaborative initiatives to address cybersecurity risks in energy systems across ASEAN. Countries have varying levels of capability, awareness, and regulatory development, which limits the effectiveness of regional cybersecurity efforts.
- Limited Awareness and Expertise: Many energy sector stakeholders, including utilities and policymakers, lack adequate awareness and expertise in cybersecurity for DES. This gap presents a challenge to the development and implementation of effective security measures.
- Cost and Investment Barriers: Investing in cybersecurity technologies and practices for DES can be cost-prohibitive, especially for developing nations within ASEAN. Without financial incentives or regional support mechanisms, there may be resistance to implementing necessary protections.

Recommendations

- Development of ASEAN-wide Basic Concept of Cybersecurity for Distributed Energy Systems: The study recommends the creation of a shared comprehensive ASEAN-wide basic concept of cybersecurity for distributed energy systems. This shared basic concept should be developed through regional collaboration and take into account the unique energy and technological landscapes of each member state.
- Promotion of Regional Cooperation and Knowledge Sharing: ASEAN nations should enhance regional cooperation by establishing forums for knowledge exchange on cybersecurity risks and best practices for DES. This will help harmonise policies, create synergies, and leverage collective expertise across the region.
- Capacity Building and Training Programmes: There is an urgent need to develop and implement training programs focused on cybersecurity for energy sector professionals. Policymakers, regulators, and energy companies must be equipped with the skills and knowledge to address evolving cybersecurity challenges in DES.
- Incentivising Cybersecurity Investments: ASEAN governments should consider providing financial incentives or regulatory support to encourage energy companies to invest in cybersecurity technologies. This can include subsidies, tax incentives, or public-private partnerships to offset the cost of implementing secure DES systems.

- Integration of Cybersecurity into National Energy Policies: Cybersecurity should be integrated into each ASEAN country's national energy policy, with a specific focus on DES and renewable energy sources. They can take reference from the Cyber Physical Security Framework (CPSF) proposed by the Ministry of Economy, Trade and Industry (METI) of Japan and customise it for their own country's context.

This study provides a roadmap for ASEAN to secure its distributed energy future, ensuring that cybersecurity is a central pillar of its energy transition. By implementing these recommendations, ASEAN can safeguard its energy infrastructure while advancing toward its sustainability and decarbonisation goals.

Project Overview

1. Project Background

The Paris Agreement calls for efforts to minimise the effects of climate change by limiting the global average temperature increase to well below 2°C and within 1.5°C of pre-industrial levels, and to this end, member countries should work together toward carbon neutrality or net zero emissions.

Southeast Asia is experiencing rapid economic growth, and energy demand is expected to increase accordingly. In Southeast Asia, distributed energy systems (DES) are also expected to contribute to decarbonisation and security of supply; a report released by ERIA in 2018 estimated investment opportunities of US$34 billion by 2040 in DERs, including solar, wind, biomass, and hydropower.

In January 2022, the Asian Zero Emission Community (AZEC) concept was launched as a partnership for Asian countries to share the idea of decarbonisation and to promote energy transition. A summit was held in December 2023, and as a result of that summit, a joint statement was issued. The Joint Statement of the AZEC Leaders' Summit listed 'expanded interregional cooperation and grid flexibility' and 'reliable microgrids utilising renewable energy in remote islands' as areas of support, and the use of distributed energy resources (DER), such as renewable energy and the construction of smart grids are expected to contribute to decarbonisation and the securing of stable energy supply.

As a result of the increased use of DERs, the risk of cyberattacks affecting energy systems is expected to increase. In addition to conventional large-scale power systems, it is also becoming more important to establish measures and mechanisms for systems related to smart grids that can also control energy resources on the consumer side in a bidirectional manner.

Currently, the IEC System Committee for Smart Energy is beginning to organise the concept of cyber security required for smart energy and smart grids based on the ERAB Security Guidelines.

2. Project Objective

The objective of this project is to work towards the multiple goals of the ASEAN region pertaining to energy security and security, decarbonisation, economic growth, cybersecurity, and continued regional cooperation simultaneously.

As the ASEAN region continues to grow rapidly in terms of both its population and economy, energy demands are also increasing. At the same time, there is also a pressing need to address the issue of carbon emissions, as countries around the world have pledged efforts towards achieving carbon neutrality sometime in the future. As such, there

is a need to push for the use of more renewable energy resources as well as new business models for the energy sector such as the energy resource aggregation business (ERAB). However, this cannot come at the expense of economic growth, as it is also equally important to ensure that each ASEAN member country is able to work towards a prosperous future. This is in line with the goals set out by the Asian Zero Emission Community (AZEC), which aim to balance economic growth with environmental and energy sustainability.

At the same time, there is also the need to address cybersecurity concerns, as technology advancements to the grid and increasing interconnection will inevitably lead to an increased attack surface area that may be vulnerable to cyberattacks. Therefore, another objective of this study is to gather information on the current state of cybersecurity efforts for DERs in the ASEAN region and provide an overview for relevant stakeholders, so that policies to achieve a safe business environment for new energy-related business models such as ERAB can be formulated. Furthermore, this study also aims to contribute to the development of an action plan to promote a common understanding (basic concept) related to energy and cybersecurity in ASEAN, so that this may lead to the creation of effective guidelines by each ASEAN member state in the future.

2.1. Project Scope

As shown in the figure below, the target countries for benchmarking have been selected based on the following requirements from the perspectives of the energy sector and the cybersecurity sector. From each region (Europe, APAC, and North America) the leading countries are selected with the following criteria from both energy and cyber security perspectives.

- Energy perspective: Countries that need grid coordination capacity and show a relatively higher VRE share.
- Cyber security perspective: Countries that have recorded higher number of cyber-attacks or threats.

On top of these quantitative indices, the presence of initiatives for strengthening cyber security for DES are also considered.

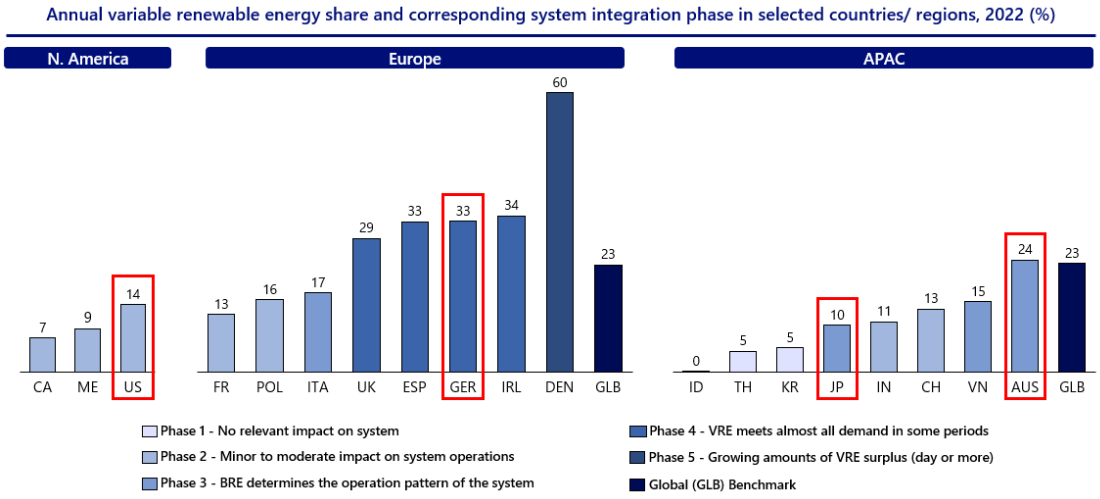
Figure 1 Selection Process of Countries

		Europe		North America	APAC	
		GER	France	USA	AUS	JP
Energy	VRE ratio	33% (3rd in Erurope)	13% (8th in Europe)	14% (Top in North America)	24% (1st in APAC)	10% (5th in APAC)
	DES-related business	EV battery related Aggregator business	Aggregator business (HEMS /ERAB)	DR Business	High potential of Aggregator business	Aggregator business (DR /ERAB)
Cyber Security	Cyber Attack (WCI)	97.41 (13th in global)	97.47 (9th in global)	100 (1st in global)	97.47 (13th in global)	97.82 (7th in global)
	CS4DES Initiative	The German Cybersecurity Act (IT-Sicherheitsgesetz)	Advanced initiative regarding household IoTs (HEMS)	Cybersecurity Baselines for DES and DER	Australian Energy Sector Cyber Security Framework (AESCSF)	ERAB Cyber Security Guideline

Source: Created by authors.

In conclusion, the US, Germany, and Australia rank amongst the top in annual VRE share and they are also amongst the most advanced in terms of corresponding system integration phases in their respective region. In terms of VRE share, Germany is in third place in Europe, followed by Denmark. In the APAC region, Australia stands at the top with the highest VRE share.

Figure 2. Annual Variable Renewable Energy Share and Corresponding System Integration Phase in Selected Countries/ Regions



Source: Created by authors based on IEA[1].

From the perspective of Cyber security according to the Global Cyber Security Index, the US ranked top, followed by Japan in 7th and France in 9th place.

[1] IEA (2024), Annual variable renewable energy share and corresponding system integration phase in selected countries/regions, 2022. https://www.iea.org/data-and-statistics/charts/annual-variable-renewable-energy-share-and-corresponding-system-integration-phase-in-selected-countries-regions-2022 (accessed 26 July 2024).

Based on these findings, this research project selected the US, Germany, France, Australia, and Japan as countries for benchmarking.

Figure 3 GCI (Global Cyber Security Index) Results: Global Score and Ranking

1	United States of America	100
2	United Kingdom	99.54
2	SaudiArabia	99.54
3	Estonia	99.48
4	Korea (Republic of)	98.52
4	Singapore	98.52
4	Spain	98.52
5	Russian Federation	98.06
5	United Arab Emirates	98.06
5	Malaysia	98.06
6	Lithuania	97.93
7	Japan	97.82
8	Canada	97.67
9	France	97.6
10	India	97.5
11	Turkey	97.49
12	Australia	97.47
13	Luxembourg	97.41
13	Germany	97.41
14	Portugal	97.32
15	Latvia	97.28
16	Netherlands	97.05
17	Norway	96.89
17	Mauritius	96.89
18	Brazil	96.6
19	Belgium	96.25
20	Italy	96.13
21	Oman	96.04
22	Finland	95.78
23	Egypt	95.48
24	Indonesia	94.88
25	Viet Nam	94.59
26	Sweden	94.55
27	Qatar	94.5
28	Greece	93.98
29	Austria	93.89
30	Poland	93.86
31	Kazakhstan	93.15
32	Denmark	92.6
33	China	92.53
33	Croatia	92.53
34	Slovakia	92.36
35	Hungary	91.28
36	Israel**	90.93
37	Tanzania	90.58
38	North Macedonia	89.92
39	Serbia	89.8
40	Azerbaijan	89.31
41	Cyprus	88.82
42	Switzerland	86.97
43	Ghana	86.69
44	Thailand	86.5
45	Tunisia	86.23
46	Ireland	85.86
47	Nigeria	84.76
48	NewZealand	84.04
49	Malta	83.65
50	Morocco	82.41
51	Kenya	81.7
52	Mexico	81.68
53	Bangladesh	81.27
54	Iran	81.07
55	Georgia	81.06
56	Benin	80.06
57	Rwanda	79.95
58	Iceland	79.81
59	South Africa	78.46
60	Bahrain	77.86
61	Philippines	77

Source: ITU.

2-1. Definition of Terms

The following table provides the definition for each of the key technical terms used in this report.

Table 1 Definition of Key Terms

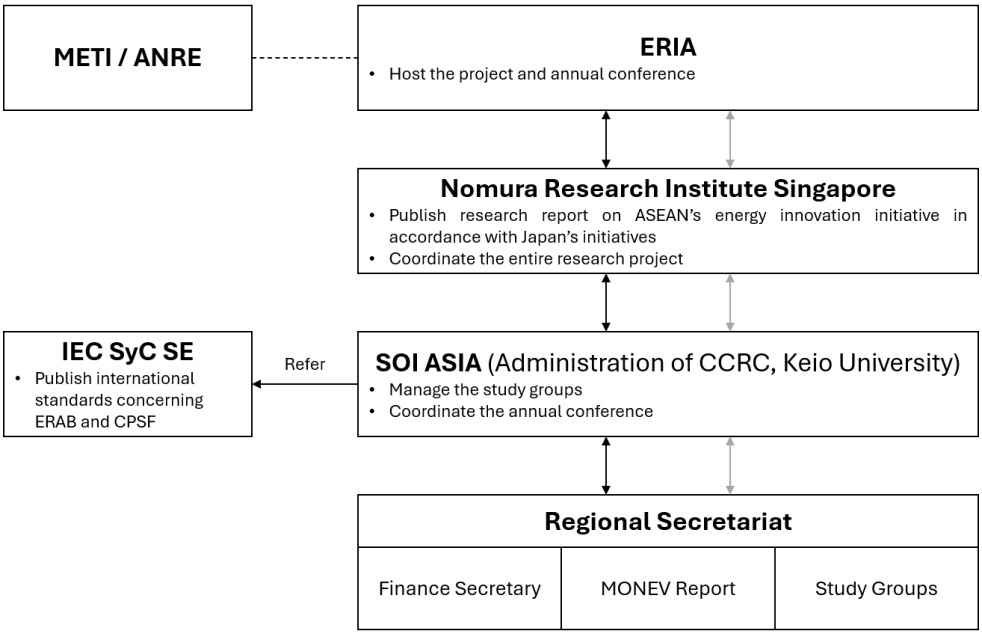
Terms	Definition
Energy Resource Aggregation Business (ERAB)	A business that provides various energy services by making use of a VPP and Demand response to electricity TSO/DSO businesses, electricity retailers, consumers, renewable-energy utilities, and other customers. (ANRE)
Distributed Energy System (DES)	A decentralised power system where electric power is produced, through renewable energy technologies or on-site generation systems, and consumed locally at or near the point of use. (ERIA)
Distributed Energy Resource (DER)	Energy resource that is located on the distribution system, any subsystem thereof, or behind a consumer's meter. (US FERC)
Distributed Energy Resource Management System (DERMS)	Software-based platform that provides the ability to continuously manage diverse and dispersed DERs, both individually and in aggregate, to support multiple objectives related to distribution grid operations, end-customer value or market participation. (IEA)

Source: Authors.

2.2. Project Structure

To achieve the abovementioned project goals, weformed a project team with SOI Asia, IEC SyC SE, as well as the Regional Secretariat to manage and facilitate the study group and conferences.

Figure 4. Project Structure

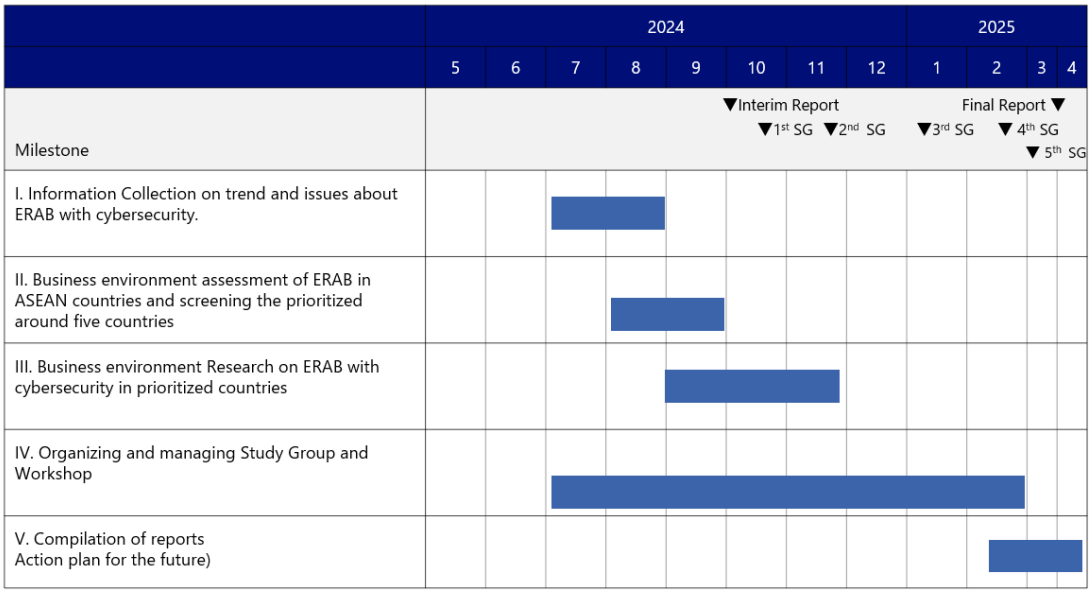


Source: Authors.

2.3. Project Timeline

The project timeline is as shown below, beginning from July 2024 and ending in April 2025. It includes 5 study groups from October 2024 to March 2025, and the Interim and Final Report submissions are scheduled for September 2024 and March 2025 respectively.

Figure 5. Project Timeline



Source: Authors

Chapter 1

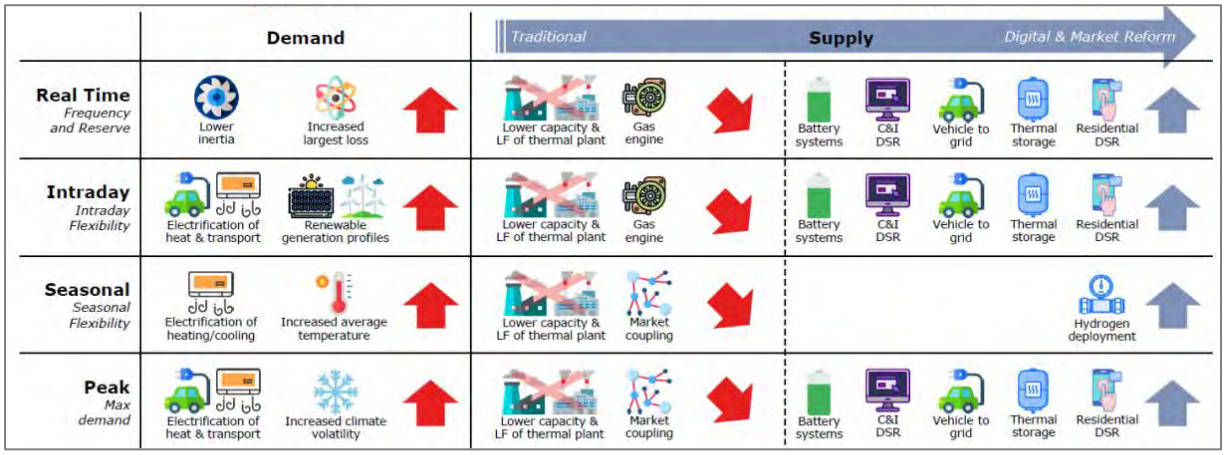
Current Progress of Adoption of Distributed Energy Resources

1. Global DES Trends

As decarbonisation for the power system progresses, distributed energy resources (DERs) will increasingly need to take on most of the flexibility requirements. In fact, the IEA's Net Zero Emission by 2050 Scenario, which limits global temperature increase to 1.5°C, indicates that more than 50% of developed countries will shift to battery storage and demand response in 2050.

The increase of installation of renewable energy and the decrease the conventional large capacity power plant, the necessity on utilisation of DER has been increased for enhancing the flexibility of the grid.

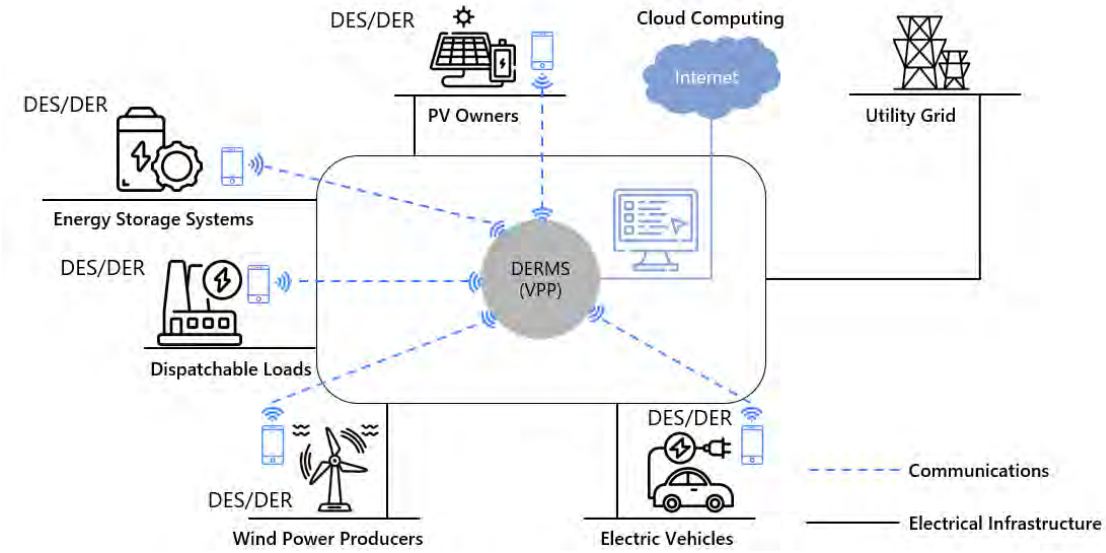
Figure 3.1 Prospects for Distributed Energy Resources



Source: IEA Electricity Security Workshop.

DES business refers to an aggregator that uses a centralised IT system (for example, cloud computing with VPP system) to remotely control the DERs, including PV, energy storage systems, dispatchable loads, wind power as well as electric vehicles, and optimise their operation.

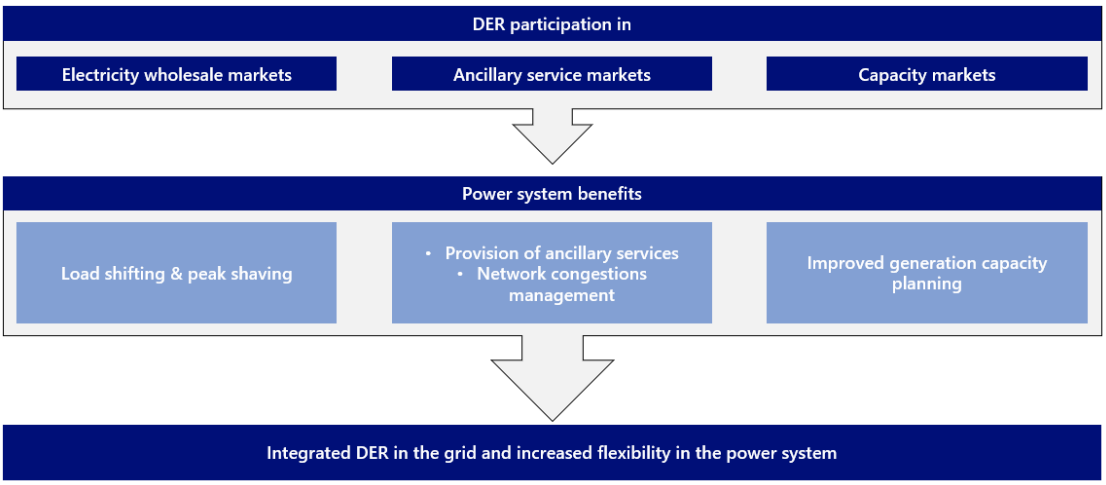
Figure 3.2 Overview of DES Business



Source: Authors.

DES/ DER could participate in the following electricity markets – electricity wholesale market, ancillary service market, and capacity market. This leads to the increase in flexibility of the total power system by providing benefits, including load shifting & peak shaving, network congestion management, and improvement of generation capacity.

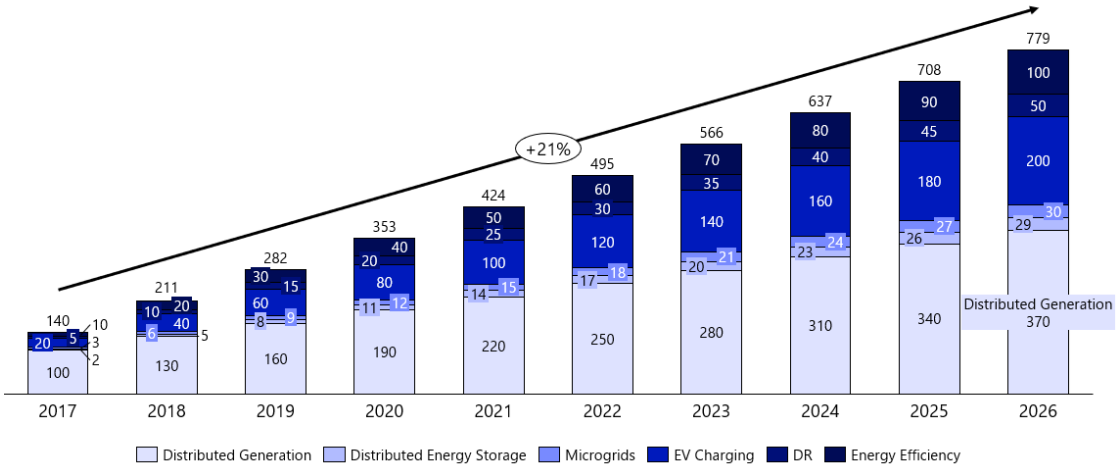
Figure 3.3 Benefits of DES/ DER



Source: Authors.

The total market size of DES globally has been forecasted to rapidly increase at 21% CAGR between 2017 and 2026.

Figure 3.4 DES Penetration Rate, Annual Installed Total DER Capacity by Technology, World Market FY2017–FY2026 ('000 MW)



Source: Created by authors based on Navigant Research[2].

To maximise the use of DER, it is necessary to promote the use of DER in conjunction with markets and distribution systems with the following approaches, as the business environment for energy aggregation business is a key success factor. Inappropriate consumer incentives may limit the potential benefits that DER can bring to the grid when the interests of DER owners and system operators are often not aligned. To avoid this outcome, regulators and system operators need to create a level playing field where DER grid contributions are properly valued, owners are fairly compensated, and system operators can more fully integrate DER services into the grid. Such coordination, when done well, will allow for more efficient deployment of financial capital and physical assets.

To improve the visibility of the power distribution system and consumer conditions, it is essential to:

- Identify data gaps, develop plans to remedy them, and increase visibility to a level that is fit for purpose
- Build a data management system that maximises the use of available data sources
- Develop a single flexible resource registry common to all market participants and explore more granular data collection options
- Improve short-term demand forecasting, dynamic network modelling, and long-term capacity planning

[2] Navigant Research (2018), Distributed Energy Resources Management Systems - Defining DERMS Use Cases and Value Propositions. https://plma.memberclicks.net/assets/resources/Navigant%20Research%20-%20AutoGrid%20DERMS%20White%20Paper.pdf (accessed 27 July 2024).

To ensure reliability and flexibility of grid connection for resources, it is essential to:

- Update grid codes to require inverter functions such as voltage/frequency ride-through and voltage regulation for DER such as distributed PV systems
- Prepare for potential challenges due to lower demand and system inertia as DER use increases
- Establish flexible grid connection requirements that reflect the impact of each resource.
- A market that actively embraces the aggregation of small-scale resources:
- Allow aggregators to participate in all markets and obtain information on benefits and risks through pilot projects
- Establish a system to compensate retailers for the roles and responsibilities of independent aggregators, especially for energy transferred through DR activation
- Reduce minimum bids, shorten procurement and delivery periods, introduce separate products for raising and lowering bids, and introduce prequalification to avoid discrimination against small-scale resources
- Develop a market participation model that can effectively incorporate new resources, such as different resource aggregations, including storage batteries, photovoltaics, electric vehicles, smart water heaters, etc.

Lastly, compensation by the market for the various benefits of immediacy:

- Same-day and real-time markets will improve the temporal granularity of market prices by shortening trading periods
- Improve the geographic granularity of price signals through nodal pricing, flexibility markets, network charges, etc.
- Complement the value of that flexible capacity to the DER, for example, by introducing scarcity pricing complemented by capacity compensation mechanisms
- Establish market rules and coordination infrastructure that allow DERs to secure multiple revenue streams while maintaining grid reliability, including amongst transmission and distribution system operators

2. Electricity Business Environment in ASEAN

2.1. Overview of ASEAN Countries

There are three main areas of demand for DES in ASEAN: (1) responding to energy transition (replacing diesel generators etc.), (2) electrification of remote areas, and (3) responding to demand for renewable energy in specific areas. Examples for each of these are described below.

(1) To respond to energy transition:

As part of efforts related to decarbonisation, conventional generators such as diesel engines in remote areas are being replaced. From the perspective of decarbonisation, gas-fired power generation is a possible alternative to diesel when diesel cannot be used, but considering the logistics involved in transporting LNG and the need to install new infrastructure such as gas pipes, this cannot be implemented immediately. By introducing PV in combination with BESS, it would be possible to supply power as a base load 24/7.

(2) To electrify remote areas:

Against the backdrop of increasing demand for electricity in island regions, demand for electricity is also increasing in island regions. In addition, the spread of DER is being promoted as an initiative to electrify unelectrified areas (particularly island regions).

(3) To respond to growing demand for renewable energy in specific areas:

In response to the growing demand for renewable energy sources, there is a need for a system that combines rooftop solar power generation, storage batteries and DEREMS. Land developers and real estate companies are acting as aggregators, buying and selling electricity in specific regions.

Looking at the situation in the ASEAN countries from the perspective of developing the business environment necessary for the ERAB project and developing a market that can be monetised, it is possible to aggregate in specific areas in the Philippines, Thailand, and Viet Nam, but the profitability is limited. Based on the research, the following chart shows the current business environment of each leading ASEAN countries from the perspective of feasibility and profitability of DES and ERAB.

Figure 3.5 Business Environment for DES/ERAB

	Market Liberalization (Feasibility)				Market Trading (Profitability)					ERAB Environment	
		Generation	TSO/DSO	Retail		Wholesale (kWh)	Reserve (kW)	Ancillary (⊿kW)	Demand Response	Carbon Credit	Comment
PH	●	● Various Player	● NGCP and others	● Meralco and others	●	● IEMOP	● IEMOP	–	– (by 2040)	–	● Favourable condition with liberalized electricity market with electricity trading scheme.
TH	▲	● EGAT and others	× EGAT	× PEA-MEA	▲	–	–	–	▲ (Demo.)	● FTI	▲ Possible but only in specific areas such as townships or Industrial Zone.
VN	▲	● EVN and others	× NPT	× EVN	▲	● EVN	● EVN	–	– (Planning)	–	▲ Possible but only in specific areas such as townships or Industrial Zone.
MY	×	● TNB and Others	× TNB	× TNB	×	–	–	–	–	● BCX	× Not Possible.
ID	×	● PLN and Others	× PLN	× PLN	×	–	–	–	–	● IDX	× Not Possible.

Source: Created by authors based on responses obtained from expert interviews.

In terms of the business environment for DES, there is potential for smart grid business in the future in the Philippines and Indonesia because demand is expected in unelectrified areas such as islands. In other countries, the potential for DES is limited due to low electricity prices.

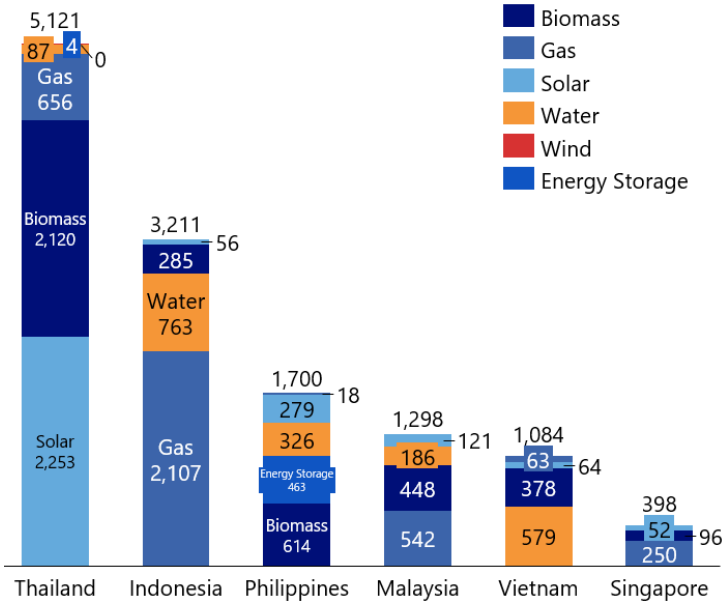
Figure 3.6 DES Business Environment in ASEAN

	DES Environment			
		DES Market Size	Electrification (Rural Area)	Issue and bottleneck
PH	●	1,700 MW	98.2%	• Regulation on Contestable customers: Only when they exceed the 500kW they can choose their own electricity contract as the contestable customer. Either meter consolidation or reduction of threshold to ramp up aggregation business. There are also some discussions to decrease the threshold. • Grid congestion and Relatively high electricity price: these factor leads further potential of expanding the business of DER or ERAB, especially in remote island.
TH	▲	5,211 MW	100%	• Lower cost of Electricity: EGAT offers electricity at a lower cost, reducing the attractiveness of DER. • Purchasing energy from neighboring: The cost of generating electricity in Thailand is too high in comparison to purchasing from neighbouring countries like Laos and Cambodia.
VN	▲	1,084 MW	100%	• Low energy tariffs : Many enterprises view energy costs as a minor expense. • No DES standards and guidance: these are not introduced yet causing adoption to be slow. • Minimal difference in costs between peak and off-peak : Despite these incentives, the difference in pricing between peak and non-peak hours might not be substantial. • No structured demand response program : This initiative involves a complex onboarding process, which can be a challenge and the lack of substantial incentives.
MY	▲	1,298 MW	100%	• Low electricity tariff and overgeneration: No appetite to pursue DES policy or programs at policy-maker level. • RE installation facilitated and reserve capacity declined : the growing interest arise when the reserves went down from 40% to 22% and the national target of 70% renewable energy penetration by 2050. . • CPPA Policy established: In September 2024, Malaysia announced 3rd party access mechanism. Now, Solar Developer can sign corporate power purchase agreement (CPPA) and pay TNB the wheeling charges. The subsequent mechanism will follow soon.
ID	●	3,211 MW	91.1%	• Industrial estate or special economic zone : Within that concession area, microgrid is responsible for generation, transmission and distribution of electricity. Majority of Microgrid players are owned by Industrial Parks company. • Demand for Renewable Energy Sources : The nature of renewable energy business in Indonesia is very spread out, where each island has its own distinguished potential of RE sources. • Grid interconnection between PLN and Non-PLN : This is the main issue from operation standpoint. Allowing PLN to determine the appropriate RE source for electricity storage can reduce the cost because RE source is a competitive advantage.

Source: Created by authors based on responses obtained from expert interviews.

Amongst the countries, Thailand and Indonesia relatively installed more DER, especially Controllable assets such as Biomass and Gas generation by installing small scale PV.

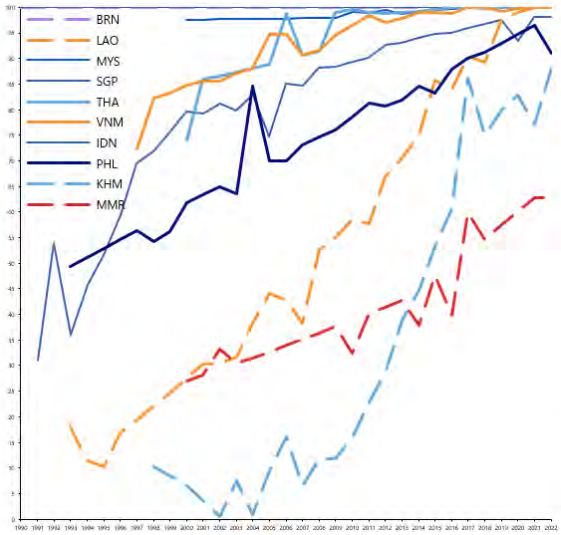
Figure 3.7 Distributed Energy Resource Installation in ASEAN



Source: Created by authors based on Capital IQ.

Amongst ASEAN Member States, Indonesia, the Philippines, Cambodia, and Myanmar still face a lack of access to electricity in rural areas. There is still some room for improvement of the rural electrification by DES.

Figure 3.8 Access to Electricity in Rural Areas (% of rural population)



(%)	2000	2010	2020	2022	CAGR
IDN	79.6	89.4	93.5	98.2	1.0%
PHL	61.8	78.5	94.7	91.1	1.8%
KHM	6.6	15.8	82.9	88	12.5%
MMR	26.9	32.5	60.1	62.8	3.9%

Source: Created by authors based on World Bank.

On top of the abovementioned analysis, the maturity analysis of power systems on ASEAN countries was conducted to clarify the difference in electricity market conditions for each ASEAN country. Based on the research, Singapore, the Philippines, Malaysia, and Thailand

were selected as Primary countries. For Cambodia, Lao PDR, Myanmar, and Brunei, where DES-related markets are not yet mature.

Table 1.1. Electricity Maturity for DES in ASEAN Countries

	Business Environment									Evaluation	
		Regulation		Bi Lateral Trading			Multi Lateral Trading				
	Evaluation	Energy System	FDI on Energy Sector	NEM / Reverse Flow	CPPA	VPPA (REC)	WESM (kWh)	Capacity (kW)	C.C. (REC)	Tier	
SG	●	●	●	●	●	●	●	●	●	1	No limitation
PH	●	●	●	●	●	●	●	●	X		
MY	▲	▲	▲	●	●	●	X	X	●	2	Only Bilateral Trading with CC Market
TH	▲	▲	●	▲	●	●	X	X	●		
ID	▲	▲	●	▲	▲	●	X	X	●	3	Limited Bilateral Trading
VN	▲	▲	●	▲	▲	●	▲	▲	X		
BU	X	X	●	●	X	X	X	X	X		
KH	X	▲	●	X	X	X	▲	▲	X	4	Difficulty for doing DES Business
LA	X	▲	●	X	X	X	X	X	X		
MM	X	▲	●	X	X	X	X	X	X		

Source: Created by authors based on responses obtained from expert interviews.

These items are evaluated based on the criteria below.

Table 1.2. Market Maturity Evaluation Criteria

	Item	Evaluation point	Evaluation Criteria
Regulation	Liberalized Energy System	What is the degree of liberalisation in the areas of generation, transmission and distribution, and sale?	Evaluated as "●" If there is liberalisation in terms of generation and sale of electricity,
	FDI for energy sector	What are the restrictions and regulations on foreign investment (FDI) in renewable energy?	Evaluated as "●" if there is no FDI regulation on renewable energy.
Bi Lateral Trading	PPA (NEM / Reverse Flow)	Is it possible to sell electricity to the grid through the Net Metering Scheme(NEM) and Reverse Flow?	Evaluated as "●" if either the NEM or Reverse Flow is in place and electricity can be sold to grid.
	CPPA	Is it possible to sell electricity to companies and consumers through the CPPA?	Evaluated as "●" if there is a system for CPPA and electricity can be sold directly to enterprises.
	VPPA（RECs）	Is it possible to trade renewable energy values or RECs with companies and customers through VPPA?	Evaluated as "●" if there is a system for VPPAs and is able to sell/buy renewable energy value directly to enterprises/users.
Multi Lateral Trading	WESM (kWh)	Does it have a Wholesale Electricity Spot Market (WES) and can kWh be traded on the market?	Evaluated as "●" if the country has a WESM market and can buy/ sell electricity on the market.
	Capacity (kW)	Does it have a Capacity Market / Reserve Market and can it trade in kW?	Evaluated as "●" if the country has a Capacity/ Reserve market and can buy/ sell on the market.
	Carbon Credit (RE)	Does it have a Carbon Credit Market, enabling market trading of renewable energy values?	Evaluated as "●" if the country has a Carbon Credit market and can be traded in the market.

Source: Created by authors based on responses obtained from expert interviews.

Table 1.3 Rooftop Solar Progress in ASEAN

Country	Rooftop Solar Potential	Current Installed Capacity	Future Installed Capacity	Key Challenges	Key Drivers
Singapore	8.6 GW	1,347.8 MW	1.5 GWp by 2025 2 GWp by 2030	The lack of space for the installation of Solar Panels Weather-issue (high humidity) affects the efficiency of Solar Panels Relatively high cost of current solar energy solutions	Grid Export for surplus electricity. (Sell the surplus electricity to SP Power Supportive policies like SolarNova Program for HDB to housing drive the demand for Rooftop PV
Indonesia	23.4 GW		3.6 GW by 2025 5.7 GW by 2028	Difficulty in attaining permits Lack of supportive incentives such as a net metering program	Renewable Energy Certificates from Rooftop Solar to obtain grants
Malaysia	4 GW	350 MW	1.1 GW by 2025	Weather-issue such as high cloud cover affects the intermittency of PV panels	Supportive programs like Net Metering Scheme to lower the cost of electricity
Philippines	40 GW	100 MW	300 MW by 2025	Relatively high cost Policy limitation and grid constraints	Supportive programs like Net Metering Scheme to lower the cost of electricity
Thailand	9 GW	1,893 MW	8.7 GW by 2037	Power market risks caused by *stop-and-go* policy Grid Connectivity issues	Supportive policies like Net Billing and Feed-in-tariffs
Viet Nam	16GW	9,500 MW	12 GWp by 2030	Lack of awareness or customer knowledge	Attractive feed-in-tariffs

				regarding the cost, efficiency and maintenance Long permit process, especially for grid connection	Ability to Sell electricity generated from rooftop PV system (partially or entire) to EVN

Source: Created by authors based on various online sources and responses obtained from expert interviews.

Table 1.4 Overview of EV Charging Stations in ASEAN

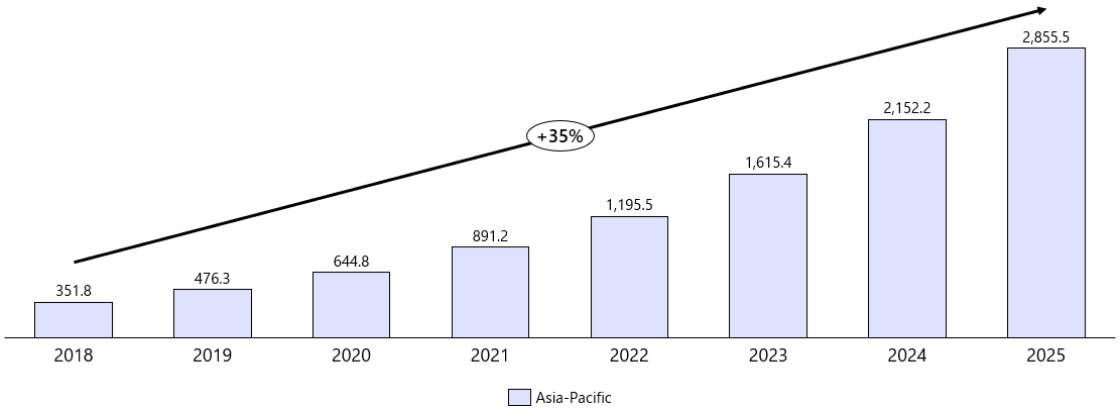
Country	Market Size for EV Charging Infrastructure	Number of EV Station	Future EV Station	Key Challenges	Key Drivers
Singapore	US$653.2 M	3,600	60,000 by 2030	Profitability issue from EV charging station operator or owner	Significant pace of EV growth will enhance the need for EV Charging station
Indonesia	US$2–3 B	3,764	32,000 by 2030	Uncertainty in government regulation regarding charging infrastructure	Establish EV Charging station in their property to attract visitors
Malaysia	*To be determined*	2,288	10,000 by 2025	Unlicensed EV Charging station that cause safety hazard (February 2024, only 223 out of 2020 public EV charging station were licensed)	Government Policy to encourage companies to build EV charging station (palm oil companies are encouraged to install and maintaining as well as providing charging services to EV owners.)
Philippines	Still very Nascent	300	7,400 by 2028	Maintaining stable supply for battery-swap	Low number of EVs which result in low number of EV

				infrastructure due to large 2-wheel EVs	charging station
Thailand	US$1.54 B	2,572	13,450 by 2030	Only available in major city like Bangkok Majority of charging station is battery-swap	Establish EV Charging station in their property to attract visitors
Viet Nam	*To be determined*	150,000	170,000 by 2025	Lack of regulation for battery production and EV Charging station	Provide subsidy of electricity prices for EV Charging station owner

Source Created by authors based on various online sources and responses obtained from expert interviews.

Asia-Pacific economies have witnessed tremendous growth in the last few years and their energy use has been increasing in recent years to meet population growth and rising standards of living.

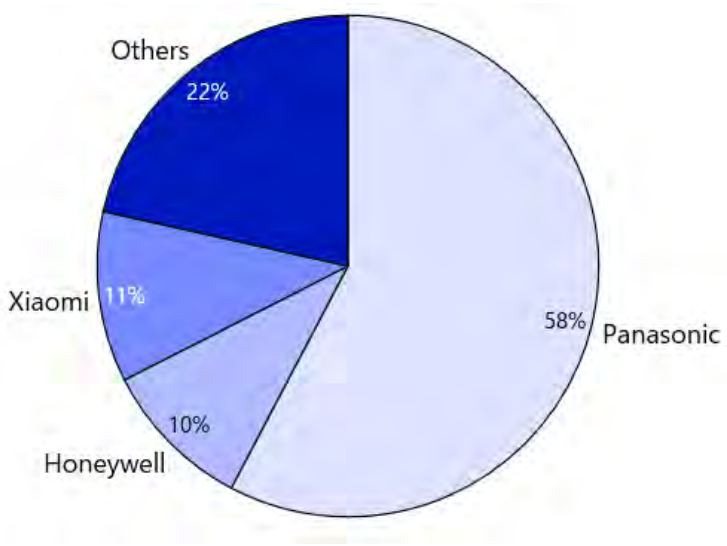
Figure 3.9 HEMS Revenue Forecast by Region, Asia-Pacific, 2018–2025



Source: Frost & Sullivan.

The Asia-Pacific HEMS market is at the growth stage, generating revenues of $351.8 million in 2018, and will grow at a compound annual growth rate (CAGR) of 35%, reaching $2,855.5 million in 2025. The market is growing because of increasing stringent compliance to energy efficiency regulations and standards requiring HEMS. Growth is expected to be mainly driven by India and China as they will account for more than half of the world's building construction between 2015 and 2030.

Figure 3.10 HEMS (%) Sales Breakdown by Region, Asia-Pacific, 2018



Source: Frost & Sullivan.

The top 3 players in HEMS makes up 78.5% of the market share with Panasonic being a significantly dominant player (58%) with strong offering of its smart home division products that covers a robust range of use cases. The HEMS distribution channel is straightforward but with increasing stakeholders as the market is slowly moving towards becoming a mass market. Direct sales and partners as a distribution structure will continue to dominate the market. These include partner providers such as home energy monitoring providers, solar energy monitoring and smart plugs providers. HEMS players seek to build long-standing relationship with customers and obtain direct access to their energy consumption data to tweak their solutions and generate more business.

Table 1.5 Southeast Asian Energy Efficiency Targets

Country	Energy Efficiency Targets
Singapore	Reduce energy intensity by 20% by 2020 and by 35% by 2030 from 2005 levels
Malaysia	Reduce final energy consumption in the industrial, commercial, and residential sectors by 10% from 2011 to 2030, and reduce final energy consumption of the transport sector by 1.4 kilo ton of oil equivalent by 2030
Indonesia	Decrease energy intensity by 1% annually and decrease energy-GDP elasticity to below 1% by 2025
Thailand	Reduce energy intensity by 25% by 2030 relative to Business As Usual (BAU)

Source: Frost & Sullivan.

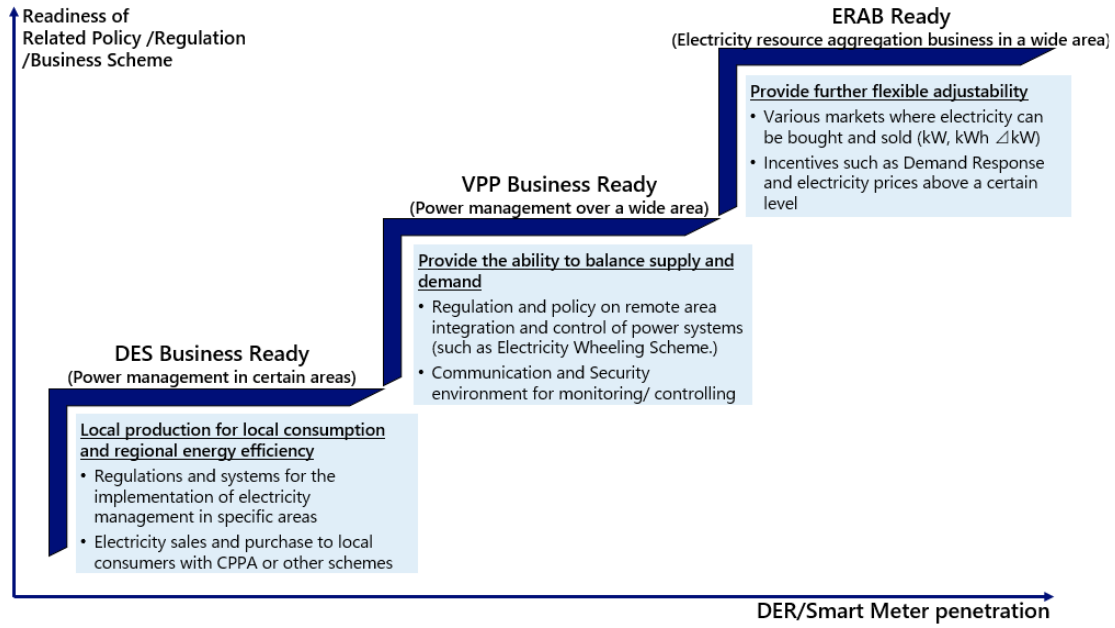
To meet the HEMS targets, Southeast Asian countries all have some form of energy efficiency targets in place, for example, energy efficiency funds, tax incentives, or in the form of minimum standards required for compliance.

3. Adoption of Distributed Energy Resources

Currently, many countries in ASEAN are at the stage where they are equipped to launch DES businesses. In other words, regulations and systems for the implementation of electricity management in specific areas are in place, and there are also schemes such as the CPPA to facilitate electricity sales and purchase.

However, many of them are still not ready for VPP or ERAB. Only Singapore is considered to be ready for VPP businesses, as it has the ability to provide balancing of supply and demand, as there are regulations and policies on remote area integration and control of power systems.

Figure 3.11 Comparison of Levels of Readiness for DES, VPP, and ERAB



Source: Created by authors.

Even though the necessary systems for the implementation of ERAB have not been implemented in ASEAN countries, the introduction of DERs and smart meters is progressing steadily. Furthermore, VPP demonstration projects are also being implemented in various ASEAN countries. Therefore, it is expected that further system development will continue to progress in the next few years. This is illustrated in the figure below.

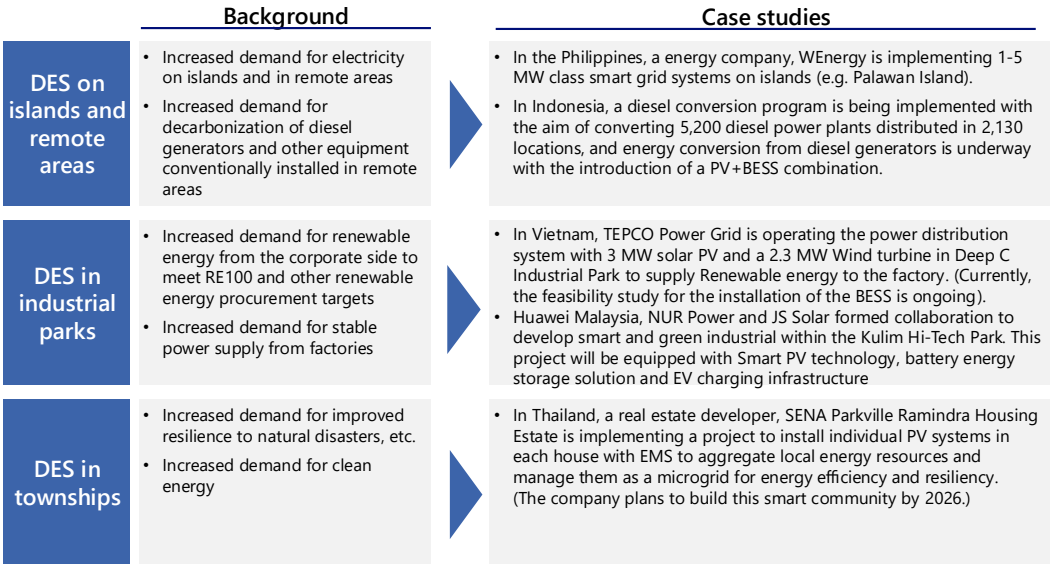
Figure 3.12 Comparison of Levels of Readiness for DES, VPP, and ERAB in ASEAN

	DES Business Ready			VPP Business Ready			ERAB Ready					DER / Smart Meter	
		Electricity Management*	CPPA		Wheeling (Off Site PPA)	VPP related Policy		Wholesale (kWh)	Reserve (kW)	Ancillary (⊿kW)	Demand Response	DER	Smart meter
	●	●	●	●	●	●	●	●	●	●	●	398 MW	95% by 2027
	●	●	●	▲	●	▲ (Demo.)	▲	●	●	×	×	1,700 MW	3.3 mil by 2024 (Meralco)
	●	●	●	▲	▲ (only Framework)	▲ (Demo.)	×	×	×	×	▲ (Demo Phase)	5,121 MW	1 mil by 2027 in MEA
	▲	●	▲ (CGPP)	▲	▲ (CGPP)	▲ (Demo.)	×	×	×	×	×	1,298 MW	9.1 mil. by 2026.
	▲	●	▲ (DPPA)	▲	▲ (DPPA)	▲ (Demo.)	×	×	×	×	×	1,084 MW	95% by 2030
	▲	▲ (Remote Area)	▲ (Limitation)	▲	▲ (Limitation)	▲ (Demo.)	×	×	×	×	×	3,211 MW	4 mil by 2025, 10 mil by 2030.

Source: Created by authors.

There are several case studies in ASEAN countries to introduce DES in islands and remote areas, industrial parks, and townships. The promotion of these initiatives can be considered as an important precursor to the future spread of DES throughout the ASEAN region.

Figure 3.13 Case Studies of DES Initiatives in ASEAN



Source: Created by authors based on various online sources.

Next, looking at the state of cybersecurity measures for the energy sector, it can be observed that cybersecurity is actually playing a limited supporting role, as they are mentioned only to a small extent in most ASEAN countries' future energy masterplans. This is summarised in the figure below.

Figure 3.14 Overview of Smart Grid/DES Masterplans in ASEAN

	Smart Grid/DES Strategy	Target for 2025-2035
ASEAN (ACE)	APAEC 2016-2025 (ASEAN Plan of Action for Energy Cooperation)	Increasing infrastructure investment into smart grid with increasing distributed RE systems usage to achieve 35% share of RE in ASEAN
	No Specific policy for smart-grid	Leverage modelling and simulations to optimize digital solutions for distribution for smart grid (National Grid Digital Twin)
	Smart Distribution Utility Roadmap (SDUR)	Improve Advanced Metering Infrastructure (AMI) through usage of SCADA and DMS as well as scale up deployments of AMI nationwide
	National Smart Grid Development Master Plan	Full-scale deployment of smart grid technologies for nominal operations and Installation and utilization of smart grid nationwide
	No Specific policy for smart-grid (Part of Malaysia' Renewable Energy Roadmap)	Increase smart grid system flexibility with expanding smart meters to Peninsular Malaysia (Malaysia's smart grid road map was released in 2009, but not updated.)
	Vietnam Smart Grid Development (Decision 4602/QDBCT/2016)	Full deployment of SCADA and DMS system for Power Corporations and complete remote metering system for all key energy users
	PLN Smart Grid Roadmap	Establishment of AMI (Advanced metering infrastructure)and advanced control center in the Java-Bali Power system with upgrading SCADA to Wide Area Monitoring system

Source: Created by authors.

According to the 8th ASEAN Energy Outlook[3], there are various barriers to significant DES adoption by ASEAN Member States, which can be classified as the following:

- Inadequate policy and regulatory frameworks
- Financial, technical, infrastructural issues
- Insufficient market
- Bureaucratic and administrative issues

Furthermore, consumer readiness is also hindered due to the lack of technical knowledge of DES products and services, as well as a limited understanding of their cost and benefits. In addition, DES' perceived high upfront costs, low existing electricity prices, shifting legislation, and complexity in permits and connection processes also further deter adoption.

To alleviate this situation, ASEAN countries need to adopt comprehensive policy reforms, provide financial incentives, invest in grid modernisation, and educate consumers on the benefits of DES.

[3] ASEAN Centre for Energy (ACE) (2024), 8th ASEAN Energy Outlook. Jakarta. https://aseanenergy.org/wp-content/uploads/2024/09/8th-ASEAN-Energy-Outlook.pdf (accessed 17 March 2025).

4. Technology Adoption and Potential Aggregation Business – Energy Resource Aggregation Business (ERAB)

Digital technologies, especially the Internet of Things (IoT), are pivotal for the increased integration of renewable energy into the existing grid. IoT can enable real-time emissions monitoring, intelligent and remote control of grid stations, optimisation of energy generation and consumption, system diagnostics, and fault detection and correction This connectivity between DERs enabled by IoT-powered devices enhances grid efficiency and also empowers consumers to optimise their energy use by adjusting consumption patterns based on real-time pricing or grid conditions, thereby making DERs more cost-effective and reliable.

According to the 8th ASEAN Energy Outlook, digital technologies such as IoT are enabling the development of a number of emerging distributed and decentralised energy infrastructures and models such as microgrids, virtual power plants (VPPs), and peer-to-peer trading. These new business models offer higher levels of grid security, improve the integration of variable renewables, and help power suppliers and consumers to optimise their levels of supply and demand. As such, IoT is a key piece in accelerating the adoption of distributed energy systems by enhancing the scalability, reliability, and cost-effectiveness of renewable energy integration[4].

Regarding emerging business models pertaining to renewable energy, DES can serve as a precursor to the energy resource aggregation business (ERAB) model. This is observed in Japan's case[5], where since the Great East Japan Earthquake of March 2011, there was increased attention on the diffusion of distributed and consumer-side energy resources (such as solar power, stationary storage batteries, electric vehicles, ENE-FARM, and negawatts) as a new business area. In November 2015, at the Public–Private Dialogue for Future Investment, the Prime Minister issued a directive to create a negawatt trading market by 2017, which would enable the trading of a certain amount of electricity saved by utilising solar PV panels and IoT in households. To this end, there was a need to establish trading rules between companies and communications standards for the remote control of energy equipment.

Consequently, this gave birth to the ERAB concept, which envisions an integrated network of IoT-applied devices, belonging to both consumers and other stakeholders, to function as if it were a single power plant (in other words a virtual power plant, also known as 'VPP').

This network will also serve the role of balancing the overall capacity of the grid, through market mechanisms and negotiated trading. In the ERAB concept, aggregators play a

---

[4] ibid.

[5] METI (2019), Cybersecurity Guidelines for Energy Resource Aggregation Business Ver 2.0. Japan. https://www.enecho.meti.go.jp/en/category/vpp_dr/data/cybersecurity_guidelines_for_erab.pdf (accessed 24 August 2024).

central role, and various services are expected to be provided through the interconnection with various recipients, such as electricity transmission/ distribution service operators (TSOs/DSOs), electricity retailers, energy management companies operating building energy management systems (BEMS) and home energy management systems (HEMS), consumers, and renewable energy utilities companies. This interconnection amongst various ERAB stakeholders will occur via the Internet and other public networks, VPNs, leased lines, and other networks.

In particular, a major feature of the ERAB system is that energy devices, which thus far have only been used in limited contexts (within the consumers' energy environments), will be connected to external systems and networks. As a result of this connection with the external environment, the Agency for Natural Resources and Energy realised the need to implement cybersecurity measures to prevent potential cyberattacks on the electricity grid. Therefore, it established a Cybersecurity Working Group as a subordinate body of the ERAB Study Group to specifically focus on cybersecurity issues in ERAB.

As such, looking at the development of events from DES to ERAB in Japan, this development and learning can probably be applied to ASEAN countries, where the implementation of DES is steadily gaining traction.

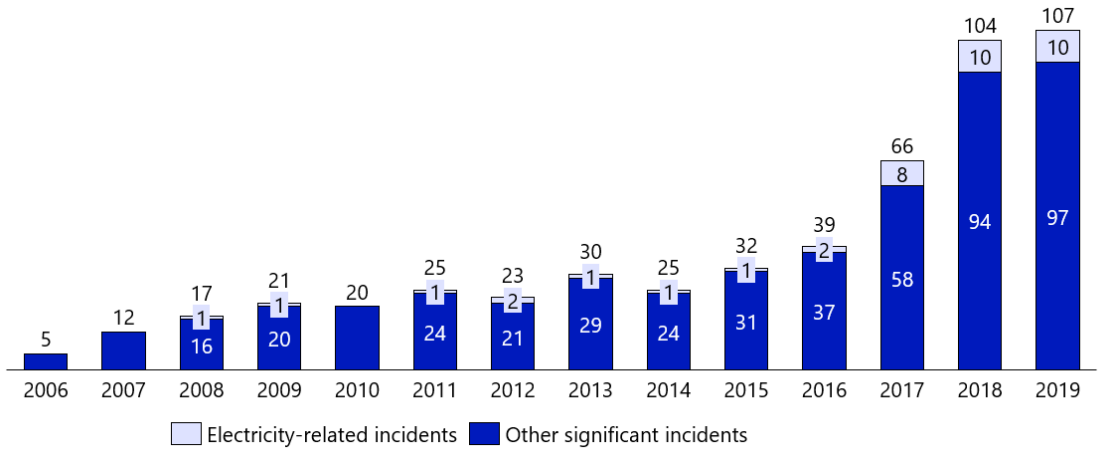
Chapter 2

Cybersecurity for Distributed Energy Systems in ASEAN

1. Global Trends of Cybersecurity Issues

There has been a consistent and sharp increase in the number of electricity-related incidents and other significant incidents from 2017–2018, as seen in the figure below.

Figure 5.1 Number of Incidents of Significant Cyber Incidents Worldwide, 2006–2019

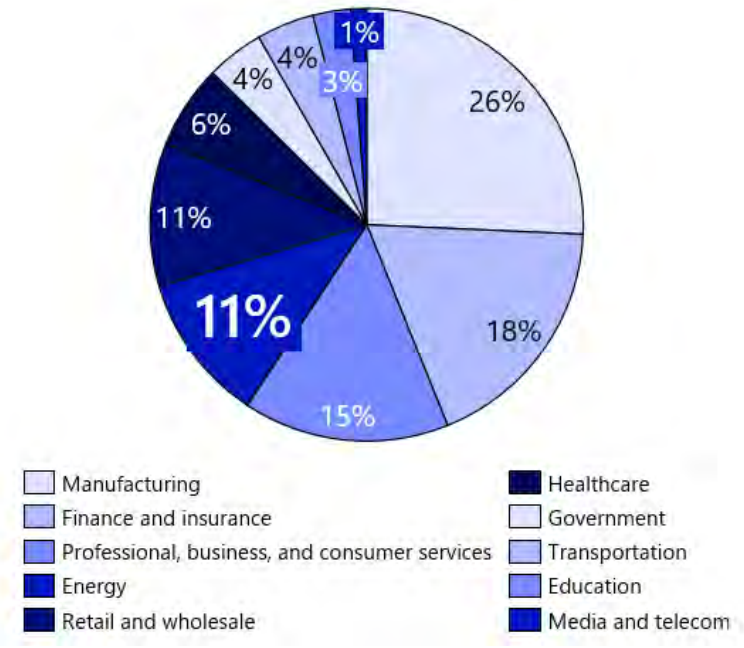


Note: 'Significant' cyber incidents are defined here as cyberattacks on government agencies, defence and high-tech companies, or economic crimes with losses of more than US$1 million.

Source: Environmental Progress & Sustainable Energy.

Manufacturing and Finance are the most targeted sectors, while the energy sector ranked fourth in the left chart. Education and Media and Telecom are the least targeted. Sectors with critical infrastructure, such as Energy, and sectors with large amounts of financial data, such as Finance and Insurance, are prominent targets for cyberattacks.

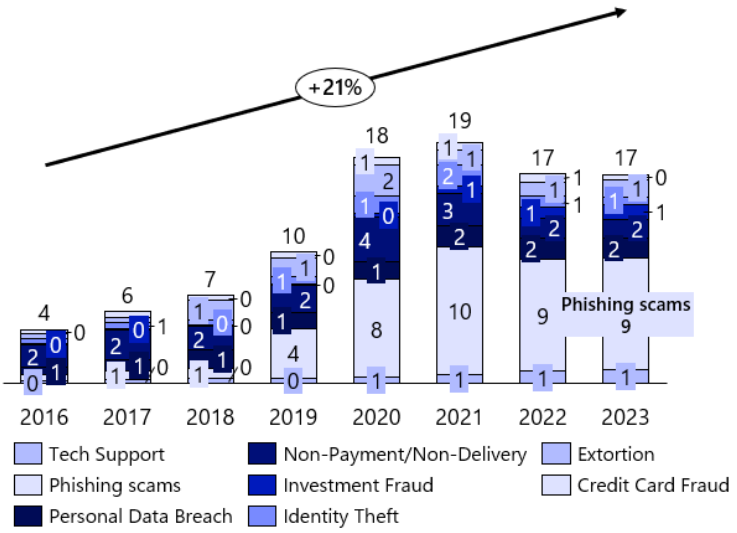
Figure 5.2 Sector Breakdown of Cyberattacks



Source: Statista.

As for the type of cyberattacks, non-payment and phishing increased during the pandemic period. Most categories also show an increase in fraud over time, particularly in investment fraud and tech support scams.

Figure 5.3 Cyberattack Volume (2016–2023), in millions



Source: Statista.

These incidents as shown in the following table highlight growing vulnerabilities in critical infrastructure and the need for enhanced cybersecurity and theft prevention measures to safeguard sensitive data and assets.

Table 2.1 Notable Cases of Cyberattacks on DES

incident	Year	summary
A suspected cyberattack disrupted Enercon's wind turbines. (Germany)	2022	• This disruption, coinciding with the Russian invasion of Ukraine, **knocked out monitoring and control systems for the turbines.** • The remote monitoring and control of **5,800 wind turbines, with a total capacity of 11 gigawatts, were knocked out.**
sPower, a renewable energy provider based in Utah, got suffer a cyber attack impacting communications with its power generation sites. (U.S)	2019	• The attack, which occurred in March 2019, exploited a vulnerability in an unpatched Cisco firewall, **causing the disconnection of sPower's wind and solar installations from its command center.** • The attack caused **temporary communication outages at several solar and wind installations** but did not affect power generation or critical control systems.
Ransomware infection in an electric power company's information system (India)	2022	• **A ransomware attack occurred at Tata Power, a power company of the Tata Group in India, resulting in the leakage of personal information such as employees' national ID card numbers**, account information, and salary information, as well as technical drawings such as blueprints and financial records, which were disclosed to the outside world.
Theft of solar panels and cables from photovoltaic facilities (Japan)	2023.	• **Solar panels and copper cables that connect panels to power conditioners and other equipment were frequently stolen from solar power generation facilities** in various locations due to break-ins. • There have also been cases where electrical accidents have been induced by the above causes, resulting in fires.

Source: Various websites, compiled by authors.

2. Overview of Cybersecurity Issues and Cybersecurity for Distributed Energy Systems in ASEAN

Figure 5.4 Overview of Cyberattack Trends in Southeast Asia

Source: Created by authors based on Kaspersky[6].

The number of cyberattacks has been rising across all Southeast Asian countries as cybercriminals become more adept at employing sophisticated tools, particularly social

[6] Manila Bulletin (2022), Six months of phishing attacks in 2022 exceed SEA's total number last year. https://mb.com.ph/2022/10/12/six-months-of-phishing-attacks-in-2022-exceed-seas-total-number-last-year/ (accessed 28 August 2024).

Cybersecurity ASEAN (2023), Malaysia Holds Top Three Spot for Phishing Attacks in Southeast Asia. https://cybersecurityasean.com/news-press-releases/malaysia-holds-top-three-spot-phishing-attacks-southeast-asia (accessed 28 August 2024).

engineering techniques, to exploit vulnerable targets. Email-based phishing attacks saw a sharp increase between 2021 and 2022, marking a concerning trend in the region. Social engineering, including phishing, has been increasingly used to manipulate individuals into revealing sensitive information or granting access to critical systems.

Kaspersky, a global cybersecurity company, reported that phishing attacks in Southeast Asia (SEA) surged dramatically during this period, with Viet Nam alone accounting for about 40% of these incidents. The region's energy sector has also become a prime target. In 2024, a dark web actor was found selling access to a major Indonesian energy company's systems, purportedly exploiting a popular cybersecurity solution used for network protection. This incident underscores the growing vulnerability of the energy sector, which is particularly concerning as it plays a critical role in national infrastructure.

Figure 5.5 Overview of Policies Related to Cyber Security for DES in Southeast Asia

	PH	TH	MY	ID	VN
Number of Cyber Threat (Phishing) ('000)	4,559	6,284	8267	4,931	17,848
Organization for promoting CS4DES	NCIAC (Not Mentioned CS4DES)	EPPO (Energy Policy and Planning Office)	NC4/ MyCERT / TNB	BSSN / CSIRT PLN	MIC / V-CERT (Not Mentioned CS4DES)
Policy on CS4DES	National Security Policy 2023-2028 (Not Mentioned CS4DES)	Master Plan for Smart Grid Network System Development (2015-2036)	Malaysia Cyber Security Strategy 2020-2024 (MCSS)	Cybersecurity control and governance in vital infrastructure	Vietnam's Digital Infrastructure Master Plan to 2030
Guideline for CS4DES	×	×	TNB Cyber Security Measures (Part of Smart Grid Initiatives)	Cybersecurity guidelines for information security management	×
Initiative or case study on CS4DES	×	×	×	PLN's management system received ISO 27001 standards for information security	×

Legend ○ : Yes △ : Partially Yes (Not of CS4DES) × : None

Source: Created by authors based on various sources.

Viet Nam (17,848) has the highest number of phishing attacks amongst these countries, followed by Malaysia (8,267), Thailand (6,284), Indonesia (4,931), and the Philippines (4,559).

The large number of cyber threats in Viet Nam and Malaysia may highlight the urgency for enhanced cybersecurity measures in critical infrastructure, including DES.

Phishing attacks are a common entry point for cybercriminals, posing significant risks to energy infrastructure.

Thailand, Malaysia, Indonesia, and Viet Nam have dedicated organisations or government bodies involved in cybersecurity efforts.

- Thailand: EPPO
- Malaysia: NC4, MyCERT, TNB
- Indonesia: BSSN, CSIRT PLN
- Viet Nam: MIC, V-CERT

Also, Malaysia, Indonesia, and Viet Nam have formal cybersecurity policies that align with their smart grid or digital infrastructure goals. Malaysia has the Cyber Security Strategy 2020–2024, highlighting specific frameworks for cybersecurity in energy systems. Indonesia focuses on cybersecurity governance in vital infrastructure, a crucial aspect of protecting energy networks like DES. Viet Nam has a Digital Infrastructure Master Plan to 2030, demonstrating its long-term vision for securing energy and other infrastructure.

The Philippines and Thailand do not have policies explicitly mentioning cybersecurity for DES. Although the Philippines has a general National Security Policy (2023–2028) which touch upon critical infrastructure, it lacks specific reference to cybersecurity for energy systems.

Furthermore, looking at the degree of liberalisation in each of the target countries, it is evident that it would be necessary to strengthen cybersecurity in the areas of system integration with businesses that are not vertically integrated. From this point of view, the Philippines requires more effort to strengthen security for external system connection points. On the other hand, other countries such as Viet Nam and Malaysia need to implement cyber security initiatives for IoT system connection to prepare for future installation of smart meters.

Table 2.2 Cybersecurity Risk Areas for ASEAN countries

	External System Connection					IoT System Connection		Evaluation
		Generation	TSO/DSO	Retail	Other market		Smart-meter	
PH	●	● Various Player	● NGCP and other DU	● Meralco and other RES	● IEMOP	▲	3.3 million smart meters by 2024 (Meralco)	Electricity is being liberalized, and interconnection with systems of multiple electric power providers has been observed; connection with IoT devices is limited, and efforts are expected to be made to evolve security, especially for connections between systems in the future.
TH	▲	● EGAT and others	× EGAT	× PEA-MEA	× PEA-MEA	▲	1 million smart meters by 2027 in MEA's area	The electric power system is composed mainly of EGAT systems, and no significant increase in the number of smart meters is expected at present.
VN	▲	● EVN and others	× NPT	× EVN	× EVN	●	95% by 2030	The electric power system is composed mainly of EVN systems, and the number of connections to external devices is expected to increase with the implementation of the DPPA system and smart meters in the future, so security measures are necessary.
MY	▲	● TNB and Others	× TNB	× TNB	N.A	●	9.1 million smart meters by 2026.	he electric power system is composed mainly of TNB systems, and the number of connections with IoT devices is expected to increase as smart meters are introduced at an accelerated pace in the future, requiring security measures.
ID	▲	● PLN and Others	× PLN	× PLN	N.A	▲	4 million by 2025, and 10 million by 2030.	The electric power system is composed mainly of PLN systems, and as smart meters are introduced at an accelerated pace in the future, the number of connections to IoT devices is expected to increase and security measures will be necessary.

Source: Created by authors based on various sources.

Each country has a different target and policy for the dissemination of smart meters, but Singapore and Malaysia are leading in this theme by targeting high ratio and number of penetration ratio of smart meter.

Table 2.3 Smart Meter Penetration Ratio and Related Initiatives in ASEAN Countries

Key Countries	Status	Target	Related initiative
SG	Mature	95% of households with smart meters by 2027	Households with smart meters will get financial incentives to cut electricity use during peak periods.
MY	Mature	9.1 million smart meters by 2026.	The initiative promotes Advanced Metering Infrastructure (AMI) as part of the "Grid of The Future" (GoTF) to advance Malaysia's energy grid towards smarter technology and improved efficiency.
PH	Emerging	3.3 million smart meters by 2024 (Meralco Target)	Meralco is piloting a smart metering system by rolling out 5,000 smart meters as part of its advanced metering infrastructure (AMI) program.
TH	Emerging	By 2027, the MEA will install 978,035 additional smart meters under AMI, while the PEA will add 70,000.	The Provincial Electricity Authority (PEA) plans to replace all meters with advanced metering infrastructure (AMI), with significant progress made.
ID	Emerging	4 million by 2025, and 10 million by 2030.	New smart meters will automate billing by wirelessly transmitting data, allowing PLN to monitor power usage in real time and reduce the need for manual inspections.
VN	Nascent	95% by 2030	The national utility has rolled out basic remote metering technologies for years with a vision to eventually transition to more advanced technologies.

Source: Created by authors based on various sources.

Cyberspace and physical space can be organised into different levels. With reference to the Purdue Model for ICS Security, levels 0 to 3 are known as the 'Operational Technology' (OT) environment, while levels 4 and 5 belong to the 'Information Technology' (IT) environment. In between levels 3 and 4 is level 3.5, which is the boundary between OT and IT systems. The table below illustrates the various equipment, networks, connections, data transfer protocols, cyber threats, and measures to deal with these threats.

Table 2.4. Operational and Information Technology Architecture and Interconnectivity

Level	IT/ OT	Main Equipment	Network	Connection with next level	Data Transfer Protocol	Cyber Threat	Measure
Level 0	OT	• Sensor • Actuators • Instrument transformers • Condition monitoring device	Local (Wired)	Copper Cable/ Fiber Optics (RJ45) / Ethernet Cables	• Modbus • DNP3	• Physical Access • Unauthorized Access	• Access Card • Guest Logbook • CCTV • Equipment lock (air-gap area)
Level 1	OT	• PLC • Intelligent Electronic Device, • Smart Inverters • managed ethernet switches,	Local (Wired)	Copper Cable/ Fiber Optics (RJ45) / Ethernet Cables	• Modbus • DNP3		
Level 2	OT	• SCADA Gateway • Enterprise Gateway • Engineering Workstation • Station-human interface	Local (Wired)	Copper Cable/ Fiber Optics (RJ45) / Ethernet Cables	• Modbus • DNP3	• Physical Access • Unauthorized Access • Data Interception • DDoS	• Encryption through public key infrastructure (PKI) • IDS (Detection), /IPS (Prevention), • Anti DDOS
Level 3	OT	• DMZ • Telecommunication Gateway	Local (Wired)	Fiber Optics / Telecom service	TCP/ IP	• Data Interception • Man in the middle attack • Network Exploits • DDoS	• Encryption via TLS or SSL • PAM (Privilege Access Management)/ PIM (Privilege Identity Management): Manages identities • Endpoint Protection: Software on servers that secures endpoints and prevents attacks via USB and external devices.
Level 3.5	IT	• Management product (firewall management, security management).	Local (Wired)	Fiber Optics / Telecom service	TCP/ IP		
Level 4	IT	• IT computer workstation Server • Web sever	Public (inc. Wireless)	Fiber Optic / Wireless	TCP/ IP	• DDoS • Application Vulnerabilities • Data Breaches • Malware, Virus	• IDS (Detection), IPS (Prevention), Anti DDOS • Patch management/ security updates • Cybersecurity awareness • anti-virus
Level 5	IT	• Application	Public (inc. Wireless)	Fiber Optic / Wireless	TCP/ IP		• :IAM (Identity Access management) • PAM (Privilege access management)

Source: Created by authors.

Next, the following table shows the overview of the international standards from IEC, ISO, and NIST that are relevant to cybersecurity for DES.

Table 2.5. Overview of Relevant International Standards

Standards	Overview	Purpose
IEC 62351	A set of standards addressing security for power system management and associated information exchange.	Protects the communication protocols used in power systems (such as SCADA) to ensure integrity, confidentiality, and authentication of messages.
IEC 61850	It relates to communication networks and systems in substations.	Facilitates interoperability of automation devices used in substations, focusing on standardizing communications between devices in energy automation systems.
IEC 62443	A comprehensive series of standards addressing cybersecurity for Industrial Automation and Control Systems (IACS).	Provides a framework for implementing secure industrial control systems (ICS), covering the entire lifecycle from risk assessment to maintenance and incident response.
IEC 60870-104	Part of the IEC 60870 series, defining telecontrol protocols for remote control of industrial processes.	Specifies the use of network protocols in SCADA systems for the transmission of process data over TCP/IP networks, focusing on energy utilities.
ISO 27000-1	An international standard for establishing, implementing, maintaining, and continuously improving an Information Security Management System (ISMS).	Ensures that organizations follow a systematic approach to managing sensitive information, including risk management and security controls.
ISO 27000-2	A code of practice providing guidance on the implementation of information security controls specified in ISO 27001.	Offers practical advice on applying security controls for managing information security risks, aligned with the requirements of an ISMS.
NIST cyber security Standards	A voluntary framework for managing cybersecurity risks in critical infrastructure sectors, widely used across various industries.	These standards are designed to enhance the resilience of organizations against cyber threats.
NIST 800-53	Outlines security and privacy controls for federal information systems.	Provides a catalog of security and privacy controls for federal information systems, adaptable to different industries to meet cybersecurity and compliance needs.
NIST 800-82	Offers guidance on securing industrial control systems (ICS).	Recommends security measures and best practices to safeguard industrial control systems, including SCADA, DCS, and PLC environments.

Source: authors.

Lastly, the following table looks at the relevant international guidelines for each level and the status of adoption in the Philippines, Thailand, Viet Nam, Malaysia, and Indonesia. Detailed explanations on the status of cybersecurity efforts in each country is covered in the following country-specific sub-chapters.

Table 2.6 Status of Adoption of Relevant International Guidelines in ASEAN

Level	Possibility	Impact	Adapted Guideline	PH	TH	VN	MY	ID
Level 0	Low	Low	• IEC 62351 • IEC 61850	● ●	● ●	× ×	● ×	× ×
Level 1	Low	Mid	• IEC 62351 • IEC 61850	● ●	● ●	× ×	● ●	× ×
Level 2	Mid	High	• IEC 61850	●	●	×	×	×
Level 3	High	High	• IEC 61850	●	●	×	×	×
Level 3.5	High	High	• IEC 60870-104	●	×	●	●	×
Level 4	High	High	• IEC 60870-104	●	●	●	●	×
Level 5	High	High	• IEC 60870-104	●	●	●	●	×
Overall	-	-	• ISO 27000-1 • IEC62443 • NIST Standard	● ● ●	● × ●	● ● ●	● ● ●	● ● ●

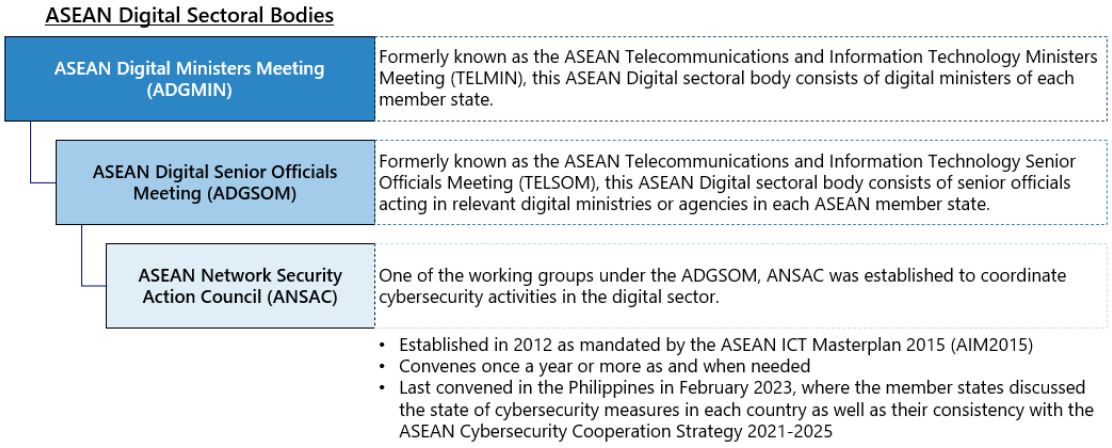
Source: Created by authors.

3. Initiatives as an ASEAN Community

3.1. Organisational Structure

ASEAN consists of different sectoral bodies which look at cybersecurity and energy separately. Cybersecurity falls under the domain of the ASEAN Digital Sector. More specifically, it is led by the ASEAN Network Security Action Council (ANSAC), which is a working group under the ASEAN Digital Senior Officials Meeting (ADGSOM).

Figure 5.6 ASEAN Network Security Action Council (ANSAC) & Higher-level ASEAN Digital Sectoral Bodies



Source: Created by authors based on information from ASEAN websites.

There are also other committees which engage in activities related to cybersecurity capacity building, digital governance, and cyber-defence. These committees are either ad-hoc working groups or closed-door meetings at the ministerial level which are involved in initiating regional cybersecurity efforts at a higher level.

Table 2.7 Overview of Other Related Cybersecurity Committees & Groups in ASEAN

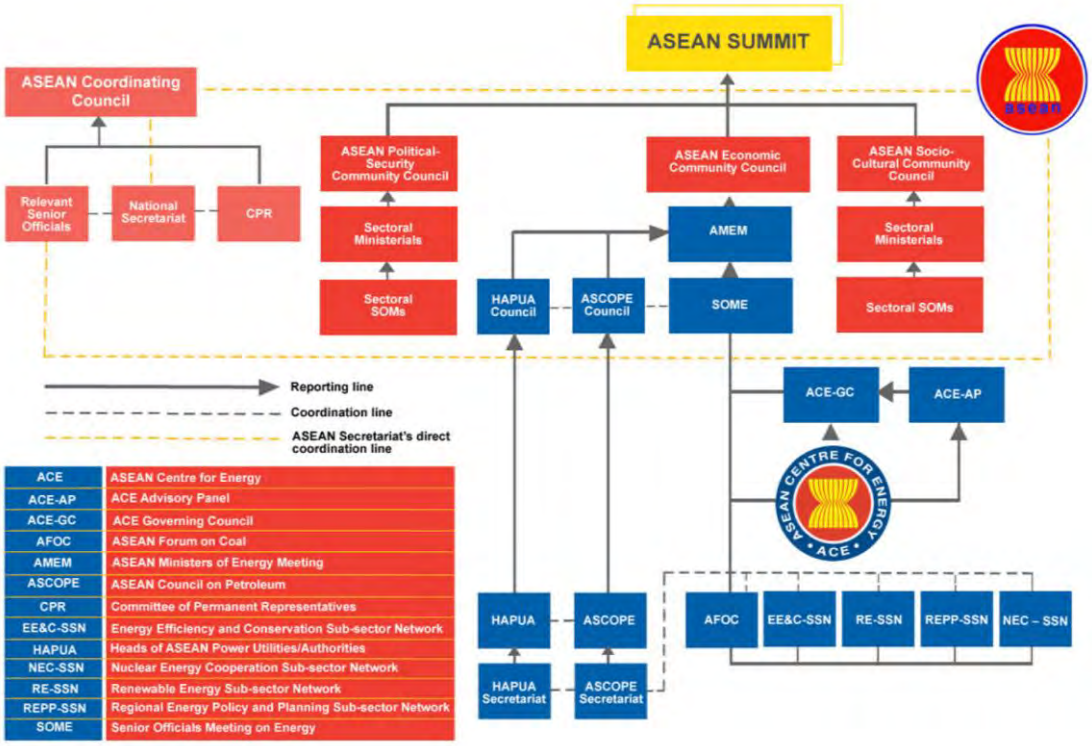
Related Cybersecurity Committees & Groups	Description	Latest Activities
ASEAN Ministerial Conference on Cybersecurity (AMCC)	Informal closed-door sessions to gather ASEAN Ministers of Telecommunications and/ or Cybersecurity. Original purpose of convening this meeting was to urge ASEAN Member States to subscribe in principle to all 11 voluntary, non-binding norms of responsible state behaviour in cyberspace according to the 2015 UN Group of Governmental Experts report.	The latest AMCC was convened in October 2023 in Singapore. Participants from all ASEAN Member States agreed on a coordinated approach to address cyberthreats, culminating in the proposal to establish the ASEAN Regional CERT. Participants also welcomed continued regional capacity building efforts by the ASEAN–Japan Cybersecurity Capacity Building Centre (AJCCBC) and the ASEAN–Singapore Cybersecurity Centre of Excellence (ASCCE).
ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC)	Comprises representatives from relevant ASEAN sectoral bodies. Set up in 2020 to strengthen cross-sectoral coordination, while preserving the exclusive work domains of the sectoral bodies.	No activities recently, after the drafting of the ASEAN Regional Action Plan on the Implementation of Norms of Responsible State Behaviour in Cyberspace (led by AMCC).
Working Group on Digital Data Governance (WG-DDG)	Ad-hoc working group under the ASEAN Digital Senior Officials Meting (ADGSOM). Established in 2018 to develop the ASEAN Framework on Digital Data Governance and implement the Framework's key initiatives.	As of 2023, the WG-DDG was working to promote the adoption of ASEAN Model Contractual Clauses, which will facilitate further integration for business and citizens. This guide will identify best practices for data transfer between ASEAN and the EU.
ASEAN Defence Ministers' Meeting (ADMM)	Highest level of meetings related to defence in ASEAN. Established in 2006 to create a defence consultative and cooperative mechanism in ASEAN. Cybersecurity efforts include the ASEAN Cyber Defence Network (ACDN) and ADMM Cybersecurity Information Centre of Excellence	Thus far in 2024, the ADMM carried out several courses on cyber incident response and threat analysis, digital defence education, and strategy paper workshops for ASEAN member state participants.

	(ACICE).	

Source: Created by authors based on various ASEAN websites and publications.

On the other hand, energy sector efforts in ASEAN are led by the ASEAN Centre for Energy (ACE). It is an ASEAN sectoral body which coordinates energy-related activities in the ASEAN region. It oversees the implementation of the ASEAN Plan of Action for Energy Cooperation (APAEC) and ensuring sustainable development in SEA.

Figure 5.7 ASEAN Centre for Energy (ACE) in the ASEAN Energy Sector



Source: ACE[7].

ACE's main role is to coordinate and support regional energy sector efforts in ASEAN by linking up different sectoral bodies with regional partners. As for ERAB/ DES, there are not many initiatives yet, because of differing regulatory landscapes in each country.

ACE's mandate is to support the implementation of regional cooperation regarding the energy sector in ASEAN such as collaboration with the Global Power System Transformation (G-PST) Consortium to host workshops for system operators to share their experiences and partnerships with the Heads of ASEAN Power Utilities/ Authorities (HAPUA). There are five working groups (WG), of which WG3 is the most relevant to this project as it handles power distribution and power quality. HAPUA WGs meet once a year.

[7] ASEAN Centre for Energy (ACE) (2024), ACE in ASEAN Energy Sector. https://aseanenergy.org/about/introduction/ (accessed 27 August 2024).

In this partnership, ACE identifies gaps of implemented action plans and bridges HAPUA with other partners under the APAEC.

ACE works under the ASEAN Plan of Action for Energy Cooperation (APAEC), which serves as the blueprint for cooperation. Under APAEC, there is the ASEAN Power Grid Initiative, and Action Plans 4.2 and 4.3 are the most relevant to DER. APAEC action plans typically last five years.

Regarding ERAB and DES initiatives in ASEAN, there are not many activities currently, and most of those which are ongoing are still in the initial stages. ACE is collaborating with ADB on the Greater Mekong Subregion to provide technical assistance and efficiency improvement for the power sector. Besides this, ACE is also identifying demand response needs and challenges from utilities operators.

The main hampering factor facing ERAB and DES initiatives is the different regulatory landscape in each country. Specifically, there is a need to protect existing utilities operators more in certain countries, as compared to those where the power sector is fully liberalised.

Besides, cybersecurity for the energy sector, let alone ERAB and DES, is not a topic that is discussed much in ASEAN, because the focus is on building more smart grid infrastructure and implementing it. Cybersecurity may appear as a topic for discussion occasionally, however there is no strong emphasis on it. For example, at each HAPUA WG meeting, the key issues faced by utilities operators are raised and discussed by the members. If one of the topics is cybersecurity, then ACE will look for the relevant ASEAN sectoral body as well as industry partners. However, so far, cybersecurity has not emerged as a key topic of discussion in these WG meetings.

The most relevant document would be Action Plan 4.3 under the APAEC. This is because Action Plan 4.3 is about the conduct of activity on power grids and cybersecurity. However, beyond the establishment of this Action Plan, there are actually not many initiatives for cybersecurity in the energy sector, let alone ERAB and DES. Cybersecurity itself is a major topic that exists separately on its own in ASEAN. There may be several cybersecurity matters that occasionally feature in discussions between HAPUA and ACE, however there are no concerted efforts focusing on cybersecurity efforts for the energy sector under ACE thus far.

Table 2.8 Overview of ASEAN Centre for Energy

Key Roles	ACE assumes a central role in the ASEAN energy sector. It works closely with energy authorities and ministries in the ASEAN Member States. It has three key roles: 1. Unify and strengthen energy cooperation within ASEAN by providing a platform for sharing, policy advisory, best practices, and capacity building 2. Provide a knowledge hub through data management, publication, and dissemination 3. Assist member states on research and identify policy solutions, legal frameworks, and new technologies

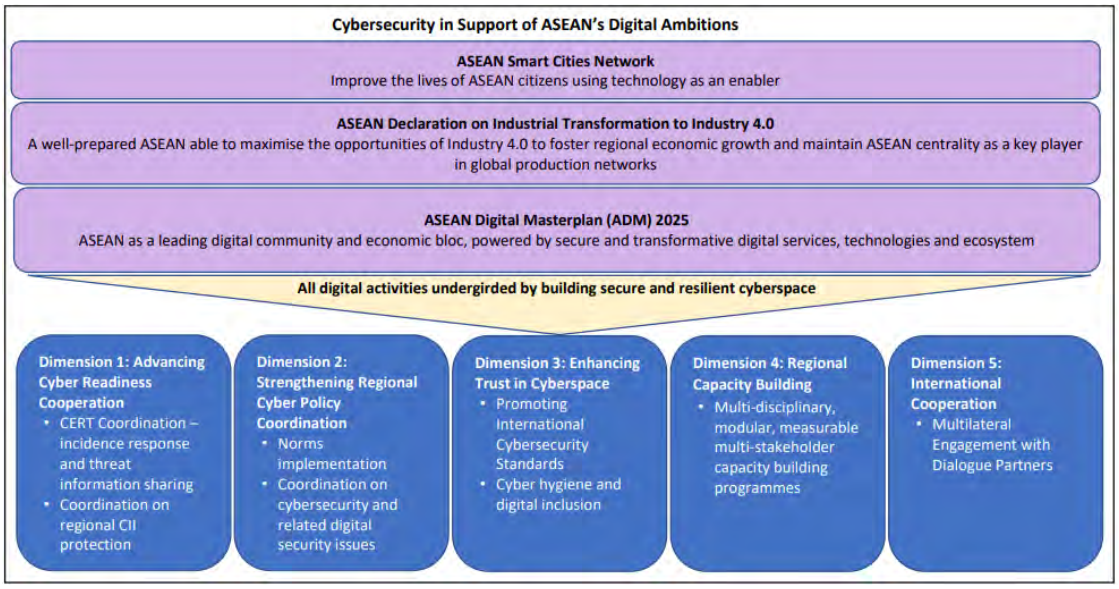
Main Actions	• Implement the ASEAN Plan of Action for Energy Cooperation • Ensure sustainable and environmentally friendly development in the ASEAN region
Reporting Structure	• ACE reports to the Senior Officials Meeting on Energy (SOME), which in turn reports to the ASEAN Ministers of Energy Meeting (AMEM)
Key Activities	• ASEAN Power Grid (APG) • Trans-ASEAN Gas Pipeline (TAGP) • Coal and Clean Technology (CCT) • Energy Efficiency and Conservation (EE&C) • Renewable Energy (RE) • Regional Energy Policy and Planning (REPP) • Civilian Nuclear Energy (CNE)

Source: Created by authors based on ACE website.

3.1. Related Policies and Initiatives

In Southeast Asia, there are cybersecurity initiatives as well as energy sector-specific initiatives undertaken by ASEAN. However, there are no cybersecurity initiatives which are specific to the energy sector per se. Instead, cybersecurity only plays a supporting role in ASEAN's other plans related to smart cities, industrial transformation (Industry 4.0), and region-wide digital cooperation. These initiatives are not binding and are also not specific to the energy-sector.

Figure 5.8 Overview of Cybersecurity Efforts in ASEAN



Source: ASEAN Cybersecurity Cooperation Strategy[8].

[8] ASEAN (2021), ASEAN Cybersecurity Cooperation Strategy (2021-2025). https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf (accessed 27 August 2024).

There are two initiatives that touch upon region-wide cyber security – the ASEAN Cybersecurity Cooperation Strategy and the ASEAN Regional Computer Emergency Response Team (ASEAN Regional CERT). These initiatives aim to create a roadmap for regional cooperation by improving cyber readiness, enhancing regional cyber policy coordination, promoting information sharing for cyber incidents.

Table 2.9 Relevant Cybersecurity Initiatives in ASEAN

Initiative	ASEAN Cybersecurity Cooperation Strategy

Description	• Roadmap for regional cooperation to create a safe and secure ASEAN cyberspace
	• Provide support different ASEAN projects
	  ○ ASEAN Smart Cities Network
	  ○ ASEAN Declaration on Industrial Transformation to Industry 4.0
	  ○ ASEAN Digital Masterplan (ADM) 2025

Main Parties	ASEAN Ministers of Telecommunications (for agreement on norms of State cyberspace behaviour)
Relevance to Cybersecurity for DES	Relevant to Industry 4.0, but no specific mention of energy sector
When	• First version released in 2017 for 2017–2020. • Second version released in 2021 for 2021–2025.
Initiative	ASEAN Regional Computer Emergency Response Team (ASEAN-CERT)
Description	• Cyber Security Agency Singapore (CSA) is proposing to establish the ASEAN Regional Computer Emergency Response Team (CERT) together with other ASEAN states to promote information-sharing for cyber incident response • The focus is on critical information infrastructure (CII) which include sectors such as banking, finance, communications, aviation, and maritime • ASEAN Digital Ministers welcomed Singapore's proposal at the 1st ASEAN Digital Ministers' Meeting in January 2021 for the establishment of an ASEAN CERT Information Exchange Mechanism
Main Parties	National-level Computer Emergency Response Teams in each ASEAN member state (for the creation of an ASEAN-wide incident response and information sharing network)
Relevance to Cybersecurity for DES	Relevant to critical information infrastructure, but no specific mention of energy sector
When	• Started in 2017. • Currently being led by Singapore. Financial model to be approved at the next Digital Ministers Meeting in 2024.

Source: Created by authors based on various ASEAN websites and publications.

Firstly, the ASEAN Cybersecurity Cooperation Strategy is a 5-year roadmap for regional cooperation to create a safe and secure ASEAN cyberspace. It will support different ASEAN projects such as the ASEAN Smart Cities Network, ASEAN Declaration on

Industrial Transformation to Industry 4.0, and ASEAN Digital Masterplan (ADM) 2025. The current (second) version of the Strategy builds upon the foundation laid by the first Strategy in incident response and capacity building cooperation. There are five key dimensions of work as shown in the following table.

Table 2.10 ASEAN Cybersecurity Cooperation Strategy and Five Key Dimensions of Work

Dimension of Work	1. Advancing Cyber Readiness Cooperation
Overview of Initiatives	• ASEAN Regional CERT Establishment • ASEAN CERT Information Exchange Mechanism Establishment • ASEAN cybersecurity threat landscape annual report • Development of ASEAN Critical Information Infrastructure Protection (CIIP) Coordination Framework
Leading ASEAN Sectoral Body	• ASEAN Network Security Action Council (ANSAC) • ASEAN Cyber CC
Dimension of Work	2. Strengthening Regional Cyber Policy Coordination
Overview of Initiatives	• ASEAN Leaders' Statement on Advancing Digital Transformation • Regional Internet Governance Forum (IGF) • Development of Matrix for ASEAN Regional Plan of Action on the Implementation of Norms of Responsible States Behaviour in Cyberspace
Leading ASEAN Sectoral Body	• ADGMIN • ATRC (together with other working groups) • ASEAN Cyber CC • ARF ISM on ICTs Security
Dimension of Work	3. Enhancing Trust in Cyberspace
Overview of Initiatives	• Development of regional cybersecurity standards for IoT • Development of regional cybersecurity policy, procedure, and guidelines for 5G and IoT implementation and Smart City implementation • Capability building activities on digital infrastructure products and software security testing and certification • Development of Cybersecurity Awareness Programme for AMS • Development of digital literacy training modules or programmes
Leading ASEAN Sectoral Body	• ANSAC • ADGSOM and ATRC • ASCN • SOMRI Working Group on IMT (WG-IMT)
Dimension of Work	4. Regional Capacity Building
Overview of Initiatives	• ASEAN–Japan Cybersecurity Capacity Building Centre's (AJCCBC) programmes

	• ASEAN–Singapore Cybersecurity Centre of Excellence's (ASCCE) programmes • ADMM Cybersecurity and Information Centre of Excellence (ACICE)
Leading ASEAN Sectoral Body	• ADGSOM + Japan • ADMM
Dimension of Work	5. International Cooperation
Overview of Initiatives	• Engagement with dialogue partners and other countries in the region for confidence building measures • CERT-to-CERT dialogues
Leading ASEAN Sectoral Body	• ARF ISM on ICTs Security, together with ASEAN Cyber CC • ANSAC

Source: ASEAN Cybersecurity Cooperation Strategy.[9]

On the other hand, the ASEAN Regional CERT was proposed to enable stronger cybersecurity incident response coordination in the region as well as improve critical information infrastructure protection cooperation.

Table 2.11 ASEAN Regional Computer Emergency Response Team (ASEAN Regional CERT)

Objectives	• Enable stronger cybersecurity incident response coordination • Improve critical information infrastructure protection cooperation (including areas such as banking and finance, communications, aviation, and maritime)
Proposed Activities	• Capacity building activities and operational coordination programmes amongst ASEAN Member States' national CERTS o Joint training sessions o Cybersecurity exercises o Networking of member states' national CERTS with Interpol, industry, and academia o Provision of industry cyber threat feeds to all ASEAN Member States
Development of Events	• First established one of the main initiatives under the first Dimension of Work in the first ASEAN Cybersecurity Cooperation Strategy (2017–2020) • Since then, the Cyber Security Agency of Singapore (CSA) has been working closely with other ASEAN states to achieve this goal. • In 2023, at the 14th ASEAN Network Security Action Council, Singapore made recommendations to host the ASEAN Regional Cert and proposed to host and fund its physical activities in Singapore • The next step is to endorse the proposed financial model to ensure sustainable funding of the ASEAN Regional CERT at the next ASEAN Digital Ministers Meeting (ADGMIN)

Source: Cyber Security Agency of Singapore.[10]

[9] ASEAN, ASEAN Cybersecurity Cooperation Strategy (2021–2025).

[10] Cyber Security Agency of Singapore (CSA) (2024), Singapore Moves Ahead to Establish the ASEAN

4. Case Studies of Cybersecurity Initiatives related to the Energy Sector, DES and ERAB in Other Countries

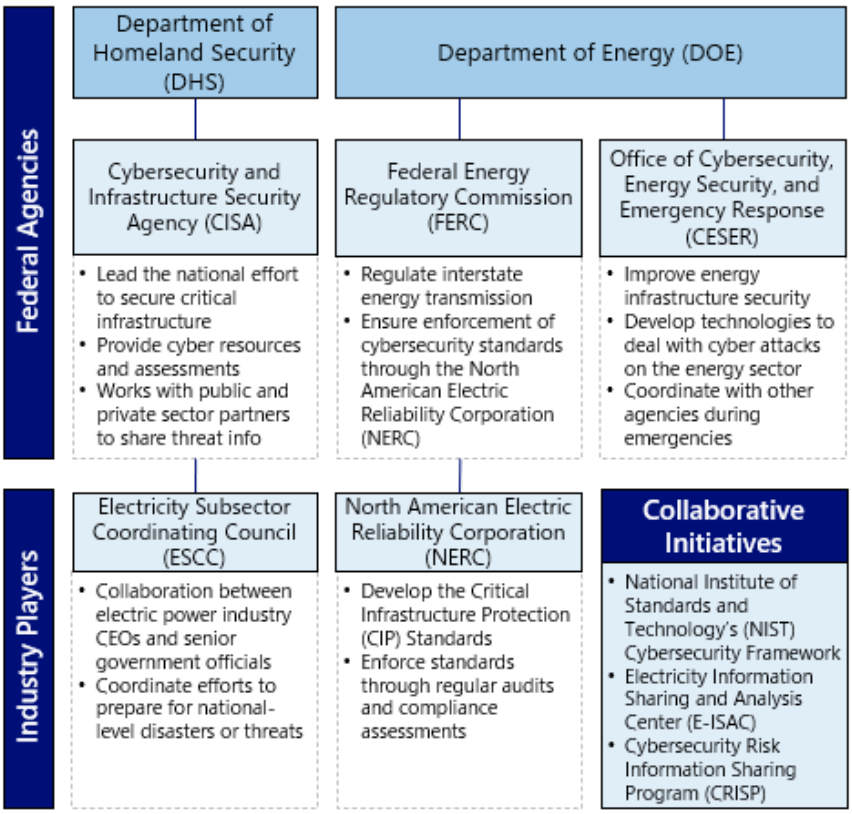
4.1. USA

Organisational Structure

Cybersecurity efforts in the energy sector in the United States involve multiple federal agencies, private sector entities, and industry associations working collaboratively. Public sector efforts are largely driven by three agencies – CISA (under the Department of Homeland Security), and the FERC and the CESER (under the Department of Energy).

Each of these agencies in turn lead various efforts and collaborate with one another as well as other public agencies and private entities to establish countrywide cybersecurity frameworks for the energy sector.

Figure 5.9 Organisation Structure of Cybersecurity for DES in the United States



Source: Created by authors based on DHS, DOE, CISA, FERC, CESER, ESCC, NERC, NIST, and E-ISAC[11]

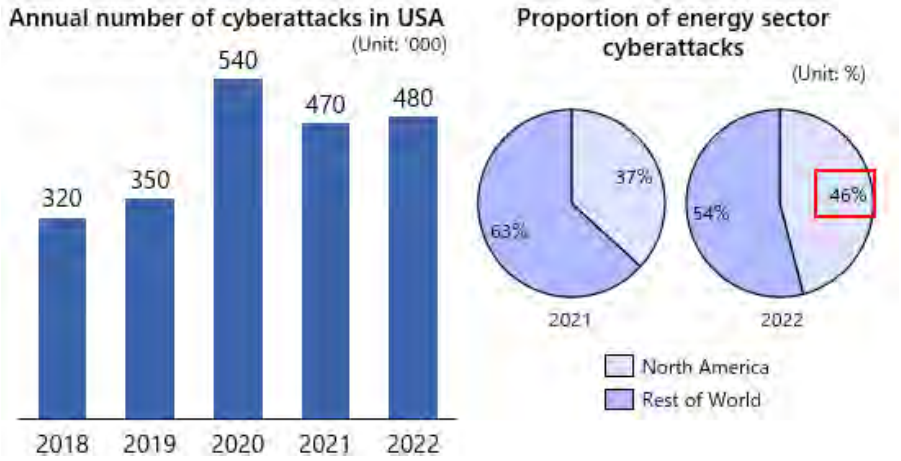
Regional CERT to Strengthen Regional Cybersecurity. https://www.csa.gov.sg/News-Events/Press-Releases/2024/singapore-moves-ahead-to-establish-the-asean-regional-cert-to-strengthen-regional-cybersecurity (accessed 27 August 2024).

[11] US Department of Energy (2024), Office of Cybersecurity, Energy Security, and Emergency Response - Authorities and Roles. Washington, DC. https://www.energy.gov/ceser/authorities-and-roles (accessed 20

Cybersecurity Incidents

In the energy sector North America was the most attacked region compared to the rest of the world in 2022, with 46% of global energy attacks taking place in North America. Notable attacks in recent years on the US energy sector include the ransomware attack on the Colonial Pipeline in 2021 which caused widespread gasoline shortages, and espionage and clandestine information gathering by Volt Typhoon (Chinese government hacking group) in 2023 where credentials were found to be stolen to enable exfiltration of valuable information on critical infrastructure.

Figure 5.10 Trend of Cyberattacks on the Energy Sector in the United States



Source: Statista, Austin Chamber[12]

August 2024).

US Department of Homeland Security (2024), About CISA. https://www.dhs.gov/keywords/cybersecurity-and-infrastructure-security-agency-cisa (accessed 20 August 2024).

Federal Energy Regulatory Commission (2024), What is FERC?. https://www.ferc.gov/what-ferc-does (accessed 20 August 2024).

Electricity Subsector Coordinating Council (2024), ESCC Overview. https://www.electricitysubsector.org/ (accessed 20 August 2024).

North American Electric Reliability Corporation (2024), About NERC. Washington, DC. https://www.nerc.com/AboutNERC/Pages/default.aspx (accessed 20 August 2024).

National Institute of Standards and Technology (2024), The NIST Cybersecurity Framework (CSF) 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (accessed 20 August 2024).

North American Electric Reliability Corporation (2024), Electricity Information Sharing and Analysis Center. Washington, DC. https://www.nerc.com/pa/CI/ESISAC/pages/default.aspx (accessed 20 August 2024).

US Department of Energy (2021), Cybersecurity Risk Information Sharing Program (CRISP). Washington, DC. https://www.energy.gov/sites/default/files/2021-12/CRISP%20Fact%20Sheet_508.pdf (accessed 20 August 2024).

[12] Statista (2024), Annual number of cyberattacks in the United States from 2016 to 2022. https://www.statista.com/forecasts/1448523/us-cyberattacks-annual (accessed 21 August 2024).

Austin Chamber (2023), We must protect our energy industry from cyberattacks – together. https://www.austinchamber.com/blog/we-must-protect-our-energy-industry-from-cyberattacks-together (accessed 21 August 2024).

In the United States, the 2020 SolarWinds hack, which was attributed to Russia, exposed major software vulnerabilities, and led to the exfiltration of information of up to 18,000 customers. In 2019, sPower faced a Denial-of-Service attack that disrupted renewable energy site communications.

Table 2.12 Notable Cases of Cyberattacks on DES in the United States

Year	Incident	Overview	Impact
2020	The SolarWinds hack, discovered involved a sophisticated attack on SolarWinds' Orion network monitoring software.	The attack, attributed to Russia, was aimed at espionage and intelligence collection, highlighting significant cybersecurity vulnerabilities in widely used software systems.	This breach gave hackers access to up to 18,000 customers, including U.S. government agencies and private organizations.
2019	sPower, a renewable energy provider based in Utah, became the first such company to suffer a cyber attack impacting communications with its power generation sites.	The attack, which occurred in March 2019, exploited a vulnerability in an unpatched Cisco firewall, causing the disconnection of sPower's wind and solar installations from its command center.	The attack caused temporary communication outages at several solar and wind installations but did not affect power generation or critical control systems.

Source: Created by authors based on various news articles.

3.2. Related Policies and Initiatives

There are two initiatives by CESER that are directly relevant to cybersecurity for DES:

- NERC's Critical Infrastructure Protection (CIP) Standards
- Cybersecurity for Energy Delivery Systems (CEDS) R&D Program

NERC's CIP Standards are governed by the Office of Cybersecurity, Energy Security, and Emergency Response (CESER), which is a sub-agency of the Department of Energy that is focused on improving energy infrastructure security and developing technologies to handle cyberattacks on the energy sector. These CIP Standards cover a wide range of items for bulk electric systems, ranging from the identification of assets to be protected to security management controls, training of personnel, and the physical and information security of assets.

On the other hand, the CEDS R&D Program, which also falls under CESER, is focused on energy delivery systems (including DERs). Under this program, CESER co-funds research projects with industry partners to develop novel cybersecurity solutions for energy delivery systems.

Separately, NARUC (together with the Department of Energy) established a set of Cybersecurity Baselines for Electric Distribution Systems and DER. This was created as

the Biden-Harris administration announced its support for electric distribution systems and distributed energy resources to enhance national and energy security for the United States as well as achieve the President's Objective of a net-zero emissions economy by 2050. These baselines form a set of recommendations which directly address cybersecurity baseline protocols for DER systems.

Table 2.13 Relevant Cybersecurity Initiatives in the United States

Policy	NERC's Critical Infrastructure Protection (CIP) Standards
Agency	CESER (under the Department of Energy)
Specific Acts	CIP-002-5.1a, CIP-003-8, CIP-004-6, CIP-005-6, CIP-006-6, CIP-009-6, CIP-011-2
Description	Identification of bulk electric system cybersecurity (BES CS); security management controls for BES CS; training of BES CS personnel; control electronic access for BES CS; physical security of BES CS; recovery plans for BES CS; information protection of BES CS
Program	Cybersecurity for Energy Delivery Systems (CEDS) R&D Program
Agency	CESER (under the Department of Energy)
Description	• Focuses on improving the cybersecurity of energy delivery systems, including DERs, through R&D, and testing of new CS technologies • CESER co-funds research projects with industry partners to develop innovative cybersecurity solutions for energy delivery systems, including DERs
Program	Cybersecurity Baselines for Electric Distribution Systems and DER
Agency	National Association of Regulatory Utility Commissioners (NARUC)
Description	• These cybersecurity baselines are a set of recommendations for electric distribution systems and the DER that connect to them. • The minimum set of cybersecurity controls is defined, but the specific procedures and technologies required are left to the implementing parties to decide.
Program	IoT Cybersecurity Improvement Act of 2020
Agency	US Congress
Description	• This Act required NIST and the Office of Management and Budget (OMB) to improve cybersecurity for IoT devices to reduce risks of these devices when connecting to federal IT systems. • As a result of this, NIST released the NIST SP 800-213 Series (IoT Cybersecurity Guidance for Federal Agencies) in December 2021
Program	NIST Cybersecurity Framework (CSF) 2.0
Authorities	National Institute of Standards and Technology (NIST)
Description	• NIST CSF 2.0 provides a structured approach to understanding, reducing and communicating cybersecurity risks • Widely adopted across various industries and has been incorporated into government policies such as the Federal Information Security Modernisation Act (FISMA), to enhance cybersecurity practices across different sectors • However, NIST CSF 2.0 does not specifically address cybersecurity for DES.

Source: DOE, NARUC, US Congress, NIST[13].

[13] US Department of Energy (2024), Cybersecurity Research, Development, and Demonstration (RD&D) for Energy Delivery Systems. Washington, DC. https://www.energy.gov/ceser/cybersecurity-research-development-and-demonstration-rdd-energy-delivery-systems (accessed 21 August 2024).

National Association of Regulatory Utility Commissioners (2024), Cybersecurity Baselines for Electric

There are two phases to the development of the Cybersecurity Baselines for Electric Distribution Systems and DER.

- Phase 1 builds on existing resources, notably the Department of Homeland Security's Cybersecurity Performance Goals (CPGs), tailored to the electric distribution sector. The process included broad stakeholder reviews to incorporate diverse perspectives.
- Phase 2 will refine and adapt the baselines based on evolving risks, technologies, and stakeholder needs.

Table 2.14 Phases of Formulation of Cybersecurity Baselines for Electric Distribution Systems and Distributed Energy Resources (DERs)

	Phase 1	Phase 2 (Future)
Approach	Creation of Cybersecurity Baselines that define essential cybersecurity controls without prescribing specific procedures or technologies. These baselines will serve as a framework for regulatory bodies and utilities to develop their own requirements.	Development of Implementation Strategies and Adoption Guidelines to assist stakeholders in applying the baselines effectively. This phase will include recommendations for assessing risks, prioritising assets, and implementing controls based on risk assessments.
Process & Development	Phase 1 built on existing resources, notably the Department of Homeland Security's Cybersecurity Performance Goals (CPGs), which were tailored for the electric distribution sector. The Steering Group leveraged these goals to create risk-informed cybersecurity practices.	Phase 2 will provide detailed implementation guidance, taking into account the diverse risks faced by different stakeholders in the distribution system. This phase will also offer suggestions for enhancing the baselines as needed.

Source: NARUC[14]

Examples of Cybersecurity Baselines for Electric Distribution Systems and DER:

- Asset Inventory
- Organisational Cybersecurity Leadership
- OT Cybersecurity Leadership

Distribution Systems and DER. Washington, DC. https://www.naruc.org/core-sectors/critical-infrastructure-and-cybersecurity/cybersecurity-for-utility-regulators/cybersecurity-baselines/ (accessed 21 August 2024).

US Congress (2020), H.R.1668 - IoT Cybersecurity Improvement Act of 2020. https://www.congress.gov/bill/116th-congress/house-bill/1668 (accessed 21 August 2024).

NIST, NIST Cybersecurity Framework (CSF) 2.0.

[14] NARUC, Cybersecurity Baselines for Electric Distribution Systems and DER.

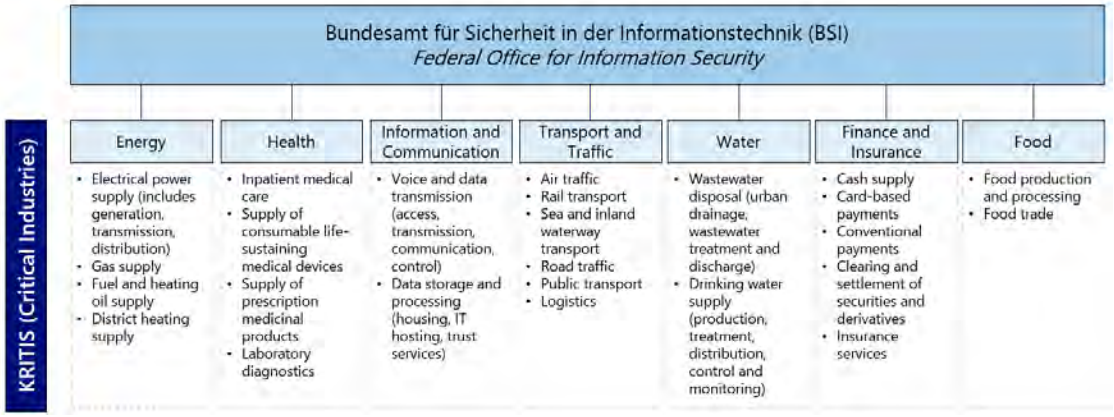
- Improving IT and OT Cybersecurity Relationships
- Changing Default Passwords
- Password Management
- Unique Credentials
- Revoking Credentials for Departing Employees
- Detecting Relevant Threats and TTPs
- Incident Reporting
- Vulnerability Disclosure/Reporting
- Incident Planning and Preparedness
- Limit OT Connections to Public Internet
- No exploitable Services on the Internet

4.2. Germany

Organisational Structure

The Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, or 'BSI') serves as the main federal body that regulates cybersecurity in critical industries ('KRITIS'). In Germany, KRITIS are organisations and facilities of significance for society whose failure or impairment would cause a sustained shortage supplies, significant disruptions to public order, safety, and security.

Figure 5.11 Critical Industries governed by the Federal Office for Information Security (BSI)



Source: Created by authors based on BSI[15]

Cybersecurity Incidents

Since 2015, operators of critical infrastructure are obliged to report disruptions that could significantly impact their functionality. In the reporting period, the BSI received 490 such reports across various sectors. The top 3 industries receiving the highest number of reports are health, transport and traffic, and energy.

Table 2.15. Number of Reports of Disruptions to Critical Infrastructure in Germany

Sector	Report
Health	132
Transport & Traffic	111
Energy	99
IT & Telecommunications	81
Finance & Insurance	61
Water	16
Food	9
Municipal Waste Management	0

Source: BSI[16]

[15] BSI (2024), KRITIS and regulated companies. https://www.bsi.bund.de/EN/Themen/KRITIS-und-regulierte-Unternehmen/kritis-und-regulierte-unternehmen_node.html (accessed 22 August 2024).

[16] BSI (2023), The State of IT Security in Germany in 2023. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2023.pdf?__blob=publicationFile&v=8 (accessed 22 August 2024).

In 2022, Germany's wind energy sector faced multiple cyberattacks, including disruptions to 5,800 turbines, and ransomware affecting Nordex's and Deutsche Windtechnik's IT systems.

Table 2.16 Notable Cases of Cyberattacks on DES in Germany

Type of DES	Type of attack	Year	Incident	Overview	Impact
Wind Turbines	-	2022	A suspected cyberattack disrupted Enercon's wind turbines.	This disruption, coinciding with the Russian invasion of Ukraine, knocked out monitoring and control systems for the turbines.	The remote monitoring and control of 5,800 wind turbines, with a total capacity of 11 gigawatts, were knocked out.
Wind Turbines	Ransomware	2022	Wind turbine maker Nordex had to shut down its IT systems across multiple locations after a cyberattack.	Conti, a notorious ransomware group, claimed responsibility for the attack, which Nordex detected early. The company shut down IT systems and disabled remote access to protect customer assets.	The shutdown affected customers, employees, and other stakeholders, but the attack was limited to Nordex's internal systems and did not impact customer assets.
Wind Turbines	Ransomware	2022	Deutsche Windtechnik, a German wind turbine maintenance company, suffered a ransomware attack.	The company manages over 7,500 turbines and has an annual turnover of $280 million, identified the attack as a targeted ransomware incident. The company managed to restore its systems without paying the ransom.	The incident forced the company to shut down its IT systems and remote monitoring connections temporarily. While the attack did not damage the turbines themselves, it did impact operational efficiency and customer service.

Source: Created by authors based on various news articles.

4.2.1.1.Related Policies and Initiatives

There are two main pieces of legislation that pertain to cybersecurity in the energy sector (and other critical industries) in Germany:

- IT Security Act (*IT-Sicherheitsgesetz*)
- Germany's National Security Strategy (*Nationale Sicherheitsstrategie*)

The IT Security Act was enacted in 2015 with the aim to enhance cybersecurity for industries with critical infrastructure. It applies to operators in sectors such as energy, water, food, and information and communications. It also empowers the BSI to be the federal advisory body for IT security as well as introduce the IT Security Mark for products. Specifically for the energy sector, it covers operators of electricity transmission grids with annual outputs of at least 3,700 GWh and district grids serving over 250,000 households. It was updated in 2016, and further revisions were made in 2021 to expand the scope of critical infrastructure sectors. As of the latest version of the Act (IT Security Act 2.0), companies operating in these sectors were required to implement attack detection systems by May 2023. Furthermore, operators are also obliged to obtain warranty declarations from manufacturers of critical components. Failure to do so could lead to fines of up to 20 million euros.

On the other hand, Germany's National Security Strategy was adopted in 2023. It serves as an integrated approach to security – covering not only military and diplomatic – but also other areas including international economics and finance, climate change, and

energy security. There are three key goals in this Strategy: robustness, resilience, and sustainability. Some key strategies include strengthening Germany's defence capabilities against various threats (including those from cyberspace), promoting technological and digital sovereignty by investing in new technologies and innovation, developing comprehensive cyber situational awareness through early warning systems, reducing critical dependencies (such as energy dependence on Russia), and improving coordination within the federal government and other authorities to repel cyberattacks.

Table 2.17 Relevant Cybersecurity Initiatives in Germany

Policy	IT Security Act 2.0 (IT-Sicherheitsgesetz 2.0)
Agency	BSI
Specific Acts	Update to IT Security Act of 2015
Description	• Expanding the scope of critical infrastructure sectors to include energy and waste management. • Introducing the category of 'companies of special public interest,' which includes defense contractors, large chemical companies, and Germany's largest companies. • Strengthening the powers and responsibilities of the Federal Office for Information Security (BSI). • Mandating the use of attack detection systems for operators of critical infrastructure by May 2023. • Requiring critical infrastructure operators to obtain warranty declarations from manufacturers of critical components. • Introducing significant fines of up to 20 million euros for non-compliance
Program	Germany's National Security Strategy
Agency	AA (Federal Foreign Office of Germany)
Description	Some key strategies include: • Strengthening Germany's defence capabilities and resilience against various threats, including those from cyberspace and hybrid warfare. • Promoting technological and digital sovereignty by investing in new technologies and innovation. • Developing comprehensive cyber situational awareness through better coordination and early warning systems, particularly involving intelligence services, with a central role in the National Cyber Response Centre. • Reducing critical dependencies in strategically relevant sectors to protect the German economy and security. • Improving coordination within the federal government and other authorities to repel cyber-attacks and enhance situational awareness in cyberspace

Source: Created by authors based on BSI and AA[17]

17 BSI (2021), Second act on increasing the security of IT systems (German IT Security Act 2.0). https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordungen/IT-SiG/2-0/it_sig_2-0.html (accessed 22 August 2024).

AA (2023), National Security Strategy. https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf (accessed 22 August 2024).

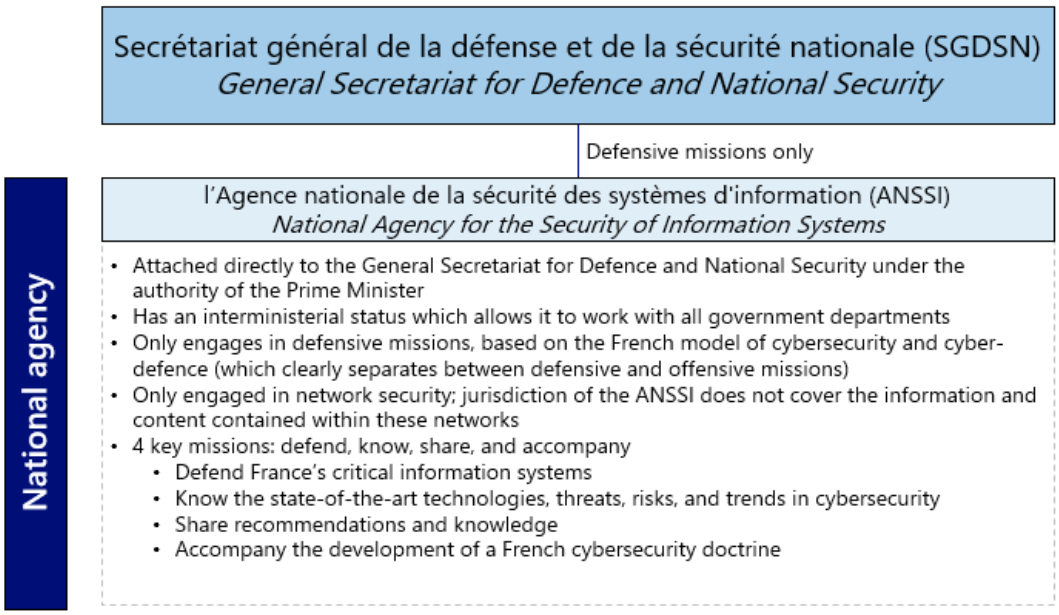
4.3. France

Organisational Structure

The National Agency for the Security of Information Systems (l'Agence nationale de la sécurité des systèmes d'information, or 'ANSSI') was created in 2009 and serves as the national authority in cybersecurity and cyber-defence. It operates under the Secretariat-General for Defence and National Security (SGDSN) and directly reports to the Prime Minister. As such, it functions as a horizontal interministerial unit that works with various government ministries and agencies as well as related partners. Under the French model of cybersecurity and cyber-defence, the ANSSI is only engaged in 'defensive missions'. The ANSSI is also only engaged in network security, meaning that its jurisdiction does not cover the information and content contained within the networks it protects. The ANSSI has four key missions:

- Defence of France's critical information systems
- Knowledge of state-of-the-art technologies, threats, risks, and trends in cybersecurity
- Sharing of recommendations and knowledge to raise awareness
- Accompaniment of the development of a French cybersecurity doctrine

Figure 5.12 Key Responsibilities of the ANSSI



Source: Created by authors based on SGDSN[18]

[18] SGDSN (n.d.), SGDSN in English. https://www.sgdsn.gouv.fr/sgdsn-english (accessed 22 August 2024).

Cybersecurity Incidents

According to the ANSSI, approximately 8% of major cybersecurity incidents specifically targeted the energy sector. This figure represents just 0.5% of the total number of incidents that targeted critical infrastructure overall. Specifically for the energy sector, there were two notable cyberattacks on the French energy provider Engie in 2023 and 2024.

Table 2.18 Notable Cases of Cyberattacks on DES in France

Overview	Year
Lapsus$ Hacker Group Compromised **Subsidiary Engie Home Services of French Energy Provider Engie** on 5 May 2024	2024
Hacktivist 'HommedeLombre' **compromised French energy company Engie and leaked personal data** of 110,000 customers on 23 August 2023	2023
Clop ransomware group exploited a zero-day in software **developer Ipswitch's MOVEit** Managed File Transfer and stole data from over 100 organisations beginning on 27 May 2023	2023
North Korean state-sponsored hacking group LABYRINTH CHOLLIMA trojanized **voice and video conferencing software 3CXDesktopApp in March 2023**	2023
Tools of cybercriminal group 'W3LL' leveraged to compromise corporate **Microsoft 365 accounts** in phishing operation beginning In October 2022	2022
Suspected Chinese threat actor UNC4841 exploited zero-day vulnerability in **Barracuda Email Security Gateway** to conduct espionage against victim organisations in at least 16 countries	2022

Source: Created by authors based on various news articles

Related Policies and Initiatives

There are two key pieces of legislation which pertain to cybersecurity in the energy sector:

- Military Programming Law (Loi de Programmation Militaire) under Law Number 703 of 2023 (Loi n° 2023-703)
- Network and Information Systems Security (NIS2) Directive under Law Number 133 of 2018 (Loi n° 2018-133)

The Military Programming Law is the most recent regulation related to cybersecurity in the energy sector. It was enacted in 2023, and it outlines defence policy and financial programming between 2024–2030, including provisions for cybersecurity. It imposes cybersecurity obligations on operators of vital importance (critical infrastructure), which include entities managing essential services in sectors such as energy, transportation, finance, and health.

On the other hand, the NIS2 Directive was enacted in 2018. It is based on the EU NIS Directive of 2016, and it requires entities to implement appropriate technical and organisational measures to manage cybersecurity risks. Significant incidents are required to be reported to the ANSSI, and operators are obliged to cooperate with regulatory authorities to ensure effective incident response. Currently, France is in the

process of transposing the updated Directive into national law.

Table 2.19 Relevant Cybersecurity Initiatives in France

Policy	Loi de Programmation Militaire (Military Programming Law)
Agency	L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
Specific Acts	LOI n° 2023-703
Description	• The most recent act is the Loi n° 2023-703, which was promulgated on August 1, 2023. This law outlines the defense policy and financial programming for the period 2024 to 2030, including provisions for cybersecurity • The LPM imposes rigorous cybersecurity obligations on operators of vital importance (OIVs), which include entities managing essential services in sectors such as energy, transportation, finance, and health. • These operators are required to implement robust security measures, conduct regular security assessments, and report significant cybersecurity incidents to the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
Program	Network and Information Systems Security (NIS) Directive
Agency	L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
Specific Acts	Loi n° 2018-133
Description	• The Network and Information Systems Security (NIS) Directive is a key piece of European cybersecurity legislation that has been transposed into French law. The original NIS Directive (Directive (EU) 2016/1148) was incorporated into French law through the Loi n° 2018-133 on February 26, 2018. • These entities are required to implement appropriate technical and organisational measures to manage cybersecurity risks, report significant incidents to the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), and cooperate with regulatory authorities to ensure effective incident response and resilience. • Currently, France is in the process of transposing the updated NIS2 Directive into national law.

Source: Created by authors based on Legifrance[19]

4.4. Australia

Organisational Structure

In Australia, cybersecurity efforts are led by the Department of Home Affairs and the Department of Defence. Their subsidiary agencies lead nationwide initiatives to secure

[19] Legifrance (2023), LOI n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense (1). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047914986 (accessed 22 August 2024).

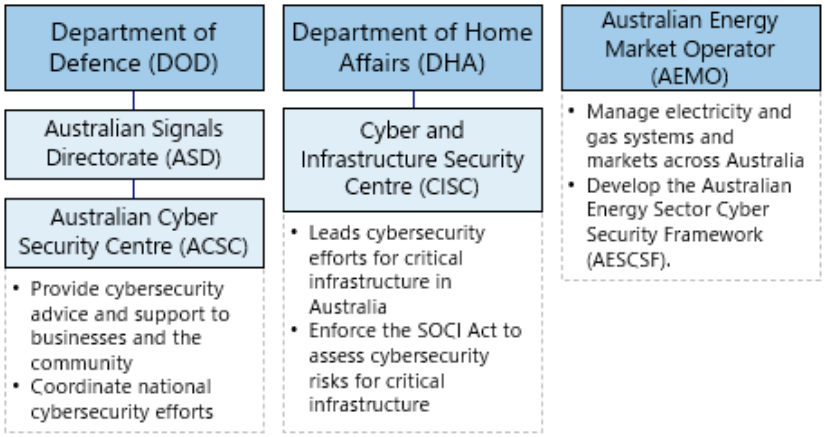
Legifrance (2018), LOI n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité (1). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000036644772 (accessed 22 August 2024).

critical infrastructure and partner with relevant stakeholders.

The Australian Cyber Security Centre (ACSC) under the Department of Defence is in charge of coordinating nationwide cybersecurity efforts, while the Cyber and Infrastructure Security Centre (CISC) under the Department of Home Affairs leads cybersecurity risk management for critical infrastructure.

As for the energy sector, the Australian Energy Market Operator (AEMO) is involved in developing a cybersecurity framework for energy industry players.

Figure 5.13 Organisation Structure of Cybersecurity for DES in Australia



Source: Created by authors based on ACSC, CISC, and AEMO[20]

Cybersecurity Incidents

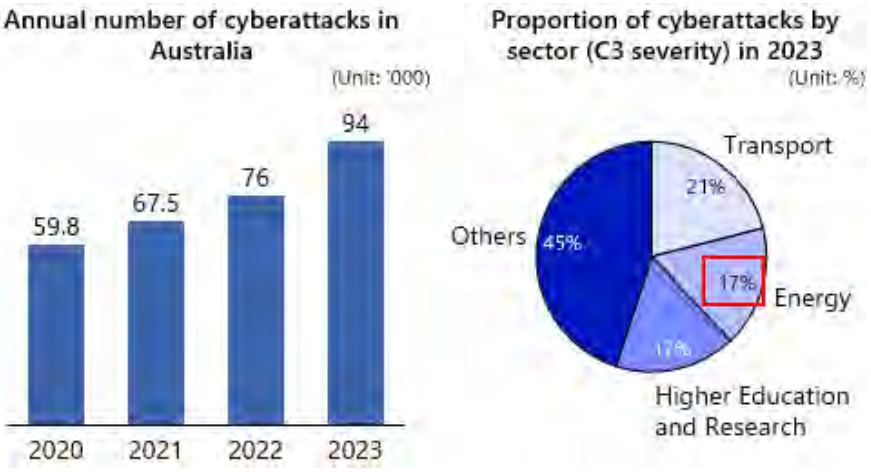
The number of cyberattacks experienced in Australia has been rising steadily. Between 2020 and 2023, the annual number of cyberattacks increased from approx. 60,000 cases to 94,000 cases. In 2023, 17% of C3 (mid-level) severity cyberattacks were on the energy sector.

[20] ACSC (2022), Who we are. Canberra. https://www.cyber.gov.au/about-us/about-asd-acsc/who-we-are (accessed 23 August 2024).

CISC (2024), About us. https://www.cisc.gov.au/about-us (accessed 23 August 2024).

AEMO (2024), AESCSF framework and resources. https://aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources (accessed 23 August 2024).

Figure 5.14 Trend of Cyberattacks on the Energy Sector in Australia



Source: Statista; Created by authors based on ASD[21]

A notable cyberattack on the energy sector happened in 2022, where Energy One, a global software provider for the energy sector, faced a ransomware attack that affected its systems in Australia and the UK.

Table 2.20 Notable Cases of Cyberattacks on DES in Australia

Type of DES	Type of attack	Year	Incident	Overview	Impact
All	Ransomware	2022	Energy One, a global software provider for the energy sector, experienced a cyberattack.	The incident affected its systems in Australia and the U.K. Energy One quickly moved to mitigate the attack's impact by disabling links between its corporate and customer-facing systems.	Impacted its corporate systems in both Australia and the United Kingdom. The company, which serves a range of clients from startups to major energy retailers and generators, took immediate action upon detecting the attack.

Source: Created by authors based on various news articles.

Related Policies and Initiatives

The key regulation which covers cybersecurity in the energy sector is the Security of Critical Infrastructure (SOCI) Act. It was enacted in 2018 and amended in 2022 to include the energy sector. It is governed by the Cyber and Infrastructure Security Centre, and it provides the framework to assess and manage security risks associated with critical infrastructure.

[21] Statista (2024), Number of cybercrime reports made to the Australian Cyber Security Centre in Australia from financial year 2020 to financial year 2023. https://www.statista.com/statistics/1343645/australia-number-of-cybercrimes-reports-acsc/ (accessed 23 August 2024).

ASD (2023), ASD Cyber Threat Report 2022-2023. Canberra. https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023 (accessed 23 August 2024).

The Department of Home Affairs oversees the overall implementation and enforcement of the SOCI Act, while the Australian Energy Market Operator (AEMO) supports enforcement within the energy sector. The Australian Cyber Security Centre (ACSC) and Cyber and Infrastructure Security Centre (CISC) provide specialised cybersecurity advice and support for critical infrastructure sectors.

Table 2.21 Relevant Cybersecurity Regulations in Australia

Policy	Security of Critical Infrastructure Act 2018 (SOCI Act)
Authorities	Cyber and Infrastructure Security Centre (CISC)
Description	Provides the framework to assess and manage security risks associated with critical infrastructure

Source: Created by authors based on CISC[22]

Besides regulatory efforts from the Department of Defence and the Department of Home Affairs, there are also other government initiatives to ensure information sharing within the energy sector as well as with other sectors. Furthermore, there are also efforts to establish cybersecurity controls for DER systems as they are integrated into the existing grid.

The Trusted Information Sharing Network (TISN) is an initiative by the CISC to enable intra-sector and cross-sector collaboration in terms of information sharing on threats, hazards, and alerts as well as useful materials and guidance.

Furthermore, there are also energy sector-specific cybersecurity initiatives such as the Australian Energy Sector Cyber Security Framework (AESCSF) and the Distributed Energy Integration Program's (DEIP) Interoperability Steering Committee. The AESCSF is a cybersecurity framework and voluntary assessment program for industry players to evaluate their cybersecurity capability and maturity. On the other hand, the DEIP Interoperability Steering Committee ensures interoperability for different IT systems, devices, and software applications (including cybersecurity applications) for the purpose of DER integration.

Table 2.22Other Relevant Cybersecurity Initiatives for the Energy Sector in Australia

Program	Trusted Information Sharing Network (TISN)
Authorities	Cyber and Infrastructure Security Centre (CISC)
Description	Besides the SOCI Act, the CISC also updated the TISN to function as a flexible network to enable cross-sector information sharing and collaboration on cybersecurity efforts with the aim of improving overall resilience capability.

[22] CISC (2024), Security of Critical Infrastructure Act 2018 (SOCI). https://www.cisc.gov.au/legislation-regulation-and-compliance/soci-act-2018 (accessed 23 August 2024).

Program	Australian Energy Sector Cyber Security Framework (AESCSF)
Authorities	Australian Energy Market Operator (AEMO)
Description	• Cybersecurity framework and voluntary assessment program for industry players. • Established in 2018, the AESCSF allows stakeholders in the energy sector to assess their own cybersecurity capability and maturity. Subsequently, they can use the results to inform and prioritise investment to improve their cybersecurity posture.
Program	Distributed Energy Integration Program (DEIP)
Authorities	Australian Renewable Energy Agency (ARENA)
Description	• Ensure interoperability for different IT systems, devices, and software applications, including cybersecurity controls for DER integration. • DEIP's main is aiming to evolve electricity grids to solve the challenges associated with increased DER. • The effort relevant to cybersecurity is carried out by the ISC, which aims to establish interoperable cybersecurity controls as part of the various integration efforts for DER systems into the existing grid.

Source: Created by authors based on CISC, AEMO, ARENA[23]

4.5. Japan

Organisational Structure

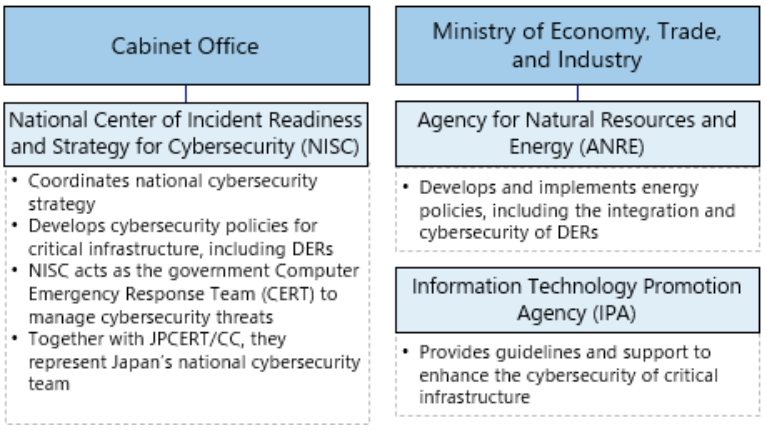
In Japan, cybersecurity for DES efforts are led by three agencies – the National Centre of Incident Readiness and Strategy for Cybersecurity (NISC) which reports to the Cabinet Office, and the Agency for Natural Resources and Energy (ANRE) and the Information Technology Promotion Agency (IPA) under the Ministry of Economy, Trade and Industry.

[23] CISC (2023), Critical Infrastructure Resilience Strategy. https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf (accessed 23 August 2024).

AEMO, AESCSF framework and resources.

ARENA (2024), Distributed Energy Integration Program (DEIP). https://arena.gov.au/knowledge-innovation/distributed-energy-integration-program/ (accessed 23 August 2024).

Figure 5.15 Organisation Structure of Cybersecurity for DES in Japan

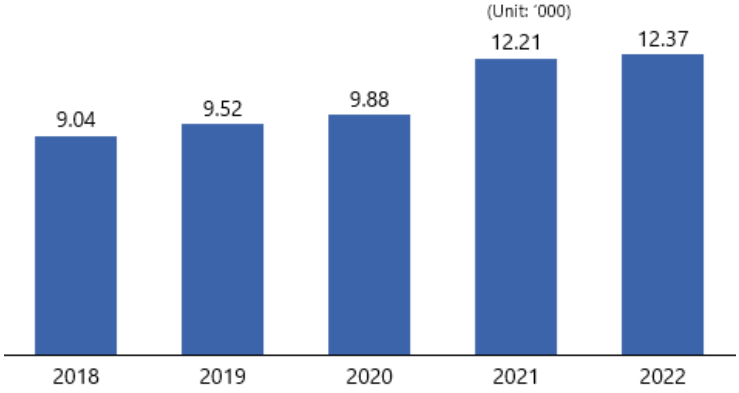


Source: NISC, ANRE, and IPA[24]

Cybersecurity Incidents

Japan has been steadily experiencing a rising number of cyberattacks, from approx. 9,000 in 2018 to approx. 12,000 in 2022. In a National Police Academy (NPA) Public Safety Survey conducted in 2022, 67.1% of all respondents answered that security in Japan had worsened, citing 'cybercrime' as one of the main causes of the deterioration.

Figure 5.16 Annual Number of Cyberattacks in Japan



Source: Statista[25]

[24] NISC (n.d.), About NISC. https://www.nisc.go.jp/eng/index.html (accessed 24 August 2024).

ANRE (2023), Policies. https://www.enecho.meti.go.jp/en/category/ (accessed 24 August 2024).

IPA (n.d.), Enabling digital transformations in industries and society. https://www.ipa.go.jp/en/digital/index.html (accessed 24 August 2024).

[25] Statista (2024), Number of cleared cybercrime cases in Japan from 2014 to 2023. https://www.statista.com/statistics/746963/japan-number-of-cyber-crime-arrests/ (accessed 24 August 2024).

In 2023, Japan experienced a significant cyberattack on its distributed energy systems. Hackers hijacked around 800 remote monitoring devices used in photovoltaic power plants, exploiting a vulnerability in Contec's SolarView Compact devices. The hackers used these devices to illegally access online banking and steal funds.

Table 2.23 Notable Cases of Cyberattacks on DES in Japan

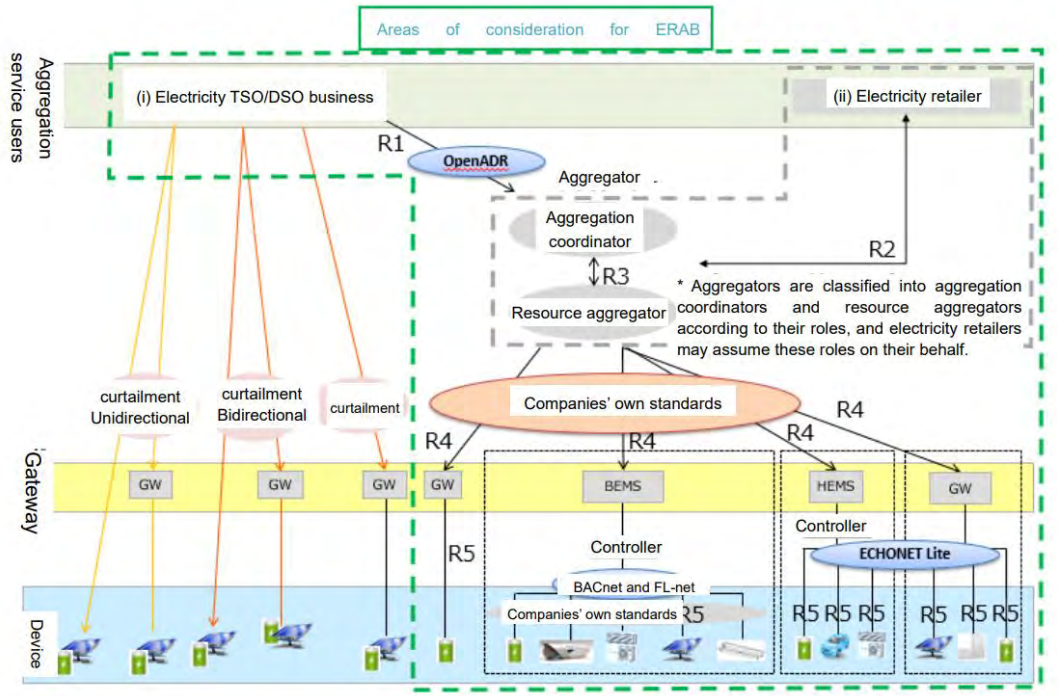
Type of DES	Type of attack	Year	Incident	Overview	Impact
Solar	Hijacking	2023	Hackers hijacked around 800 remote monitoring devices used in photovoltaic power plants, exploiting a vulnerability in Contec's SolarView Compact devices.	This attack, considered the world's first confirmed cyberattack on solar grid infrastructure, involved using these devices to illegally access online banking and steal funds.	The attackers exploited the CVE-2022-29303 vulnerability and deployed backdoor programs to manipulate the devices.

Source: Created by authors based on various news articles.

Related Policies and Initiatives

The Ministry of Economy, Trade and Industry (METI) formulated and published the Cybersecurity Guidelines for Energy Resource Aggregation Business (ERAB) in 2017 and revised it in both 2018 and 2019. These Guidelines require operators to take necessary measures to minimise risk and damage from potential cyberattacks on ERAB systems. As seen in the figure below, the ERAB system can be categorised in five layers (R1-R5). The Guidelines provide the necessary measures for each of these layers.

Figure 5.17 Areas of Consideration for Cybersecurity for ERAB

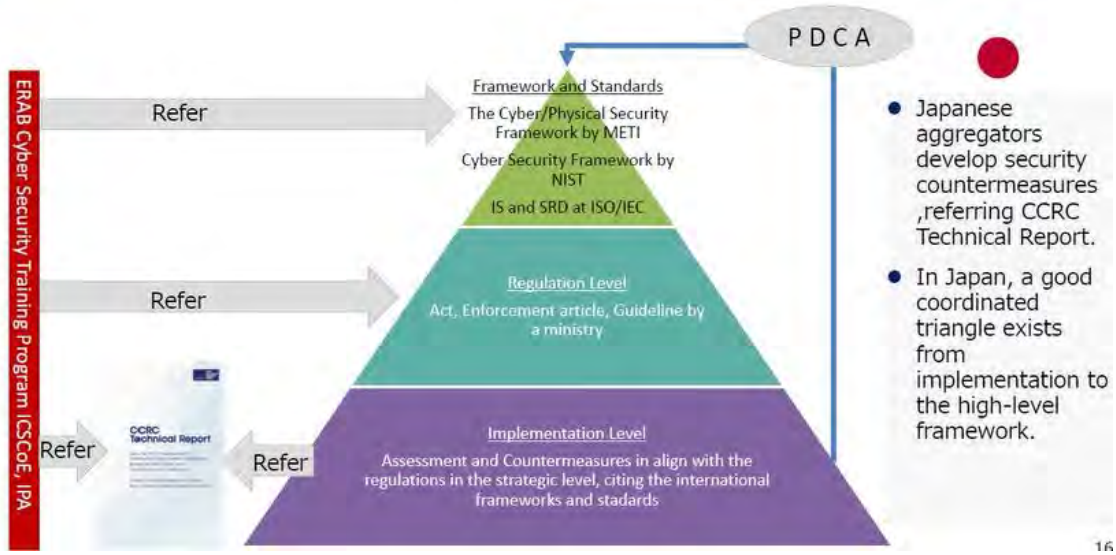


Source: METI[26]

Nonetheless, the ERAB Cybersecurity Guidelines are not legally binding, and they are just but one of several initiatives in Japan. In fact, Japanese operators and policymakers utilise a range of frameworks (including the Cybersecurity Framework by NIST as well as ISO/IEC standards) under what is known as a 'Security Triangle for ERAB in Japan'.

[26] METI, Cybersecurity Guidelines for Energy Resource Aggregation Business Ver 2.0.

Figure 5.18 Security Triangle for ERAB in Japan

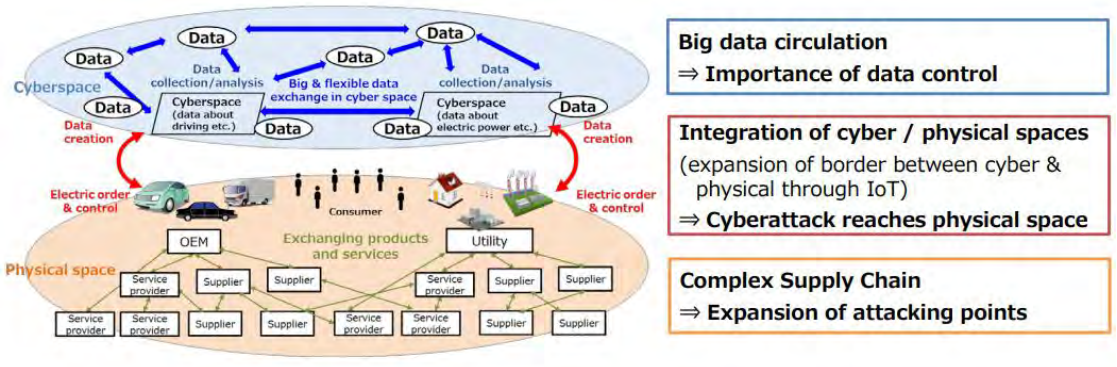


Source: METI.

As seen in the figure above, the overarching cybersecurity framework which applies across different industries is the Cyber Physical Security Framework (CPSF) by METI. This Framework was established due to the convergence of cyber and physical spaces which drastically increases the potential cyberattack surface area.

The Cyber Physical Security Framework (CPSF) was developed and published by METI in 2019. It was created as part of the Japanese government's efforts to create a next-generation smart social infrastructure programme known as 'Society 5.0'. Cybersecurity was highlighted as a key factor, due to the interconnection of cyberspace and physical space which has led to an increased impact of cyberattacks on physical infrastructure.

Figure 5.19 Overview of the Cyber Physical Security Framework (CPSF) by METI

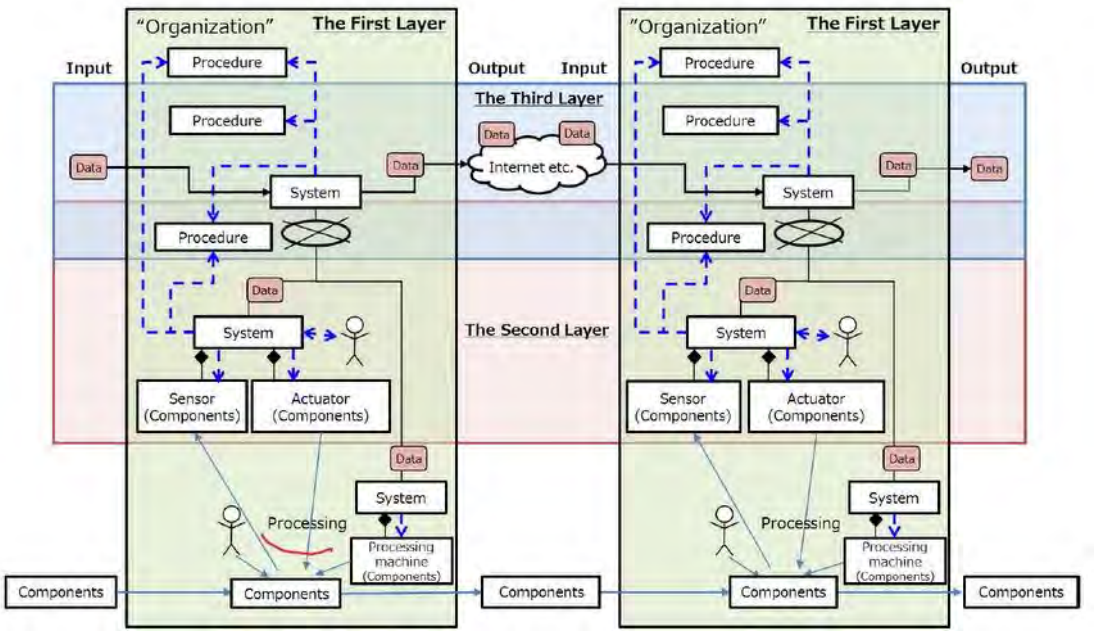


Source: METI[27]

[27] METI (2019), The Cyber/Physical Security Framework. Japan. https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0_eng.pdf (accessed 24 August 2024).

Under the CPSF, it is possible to map the six elements (organisation, people, components, data, procedures, and systems) in a three-layer model. Components communicate with actuators and sensors, which in turn communicate with their control systems. For data (internet connection) at the third layer, there is increasing communication between systems from the second and third layers (IT-OT communication). Therefore, there is a need to secure the data traversing these layers.

Figure 5.20 Three-Layer Model under the Cyber Physical Security Framework



Source: METI[28]

The first layer pertains to the creation of trust in the organisation's management. This is based on the idea that security can be through the establishment of trust within management and allowing only participants whose trustworthiness has been determined. Certification programmes such as ISMS (based on ISO/IEC 27001) can be used to create a shared security policy which serves as a basis for ensuring trust.

Next, the second layer covers the interaction between cyber and physical spaces, where physical data can be digitised, sent to cyberspace, processed and edited, analysed, and then returned to physical space. In other words, this is where the IT and OT environments converge, and IoT devices work together to connect everything to the shared network. As such, security for the second layer is based on the accuracy and trustworthiness of data transcription and transfer (including accurate translation) between cyber and physical spaces. To ensure trustworthiness in data transcription, in accordance with ISO/IEC 27036, all elements of the system life cycle, including construction and maintenance, must also

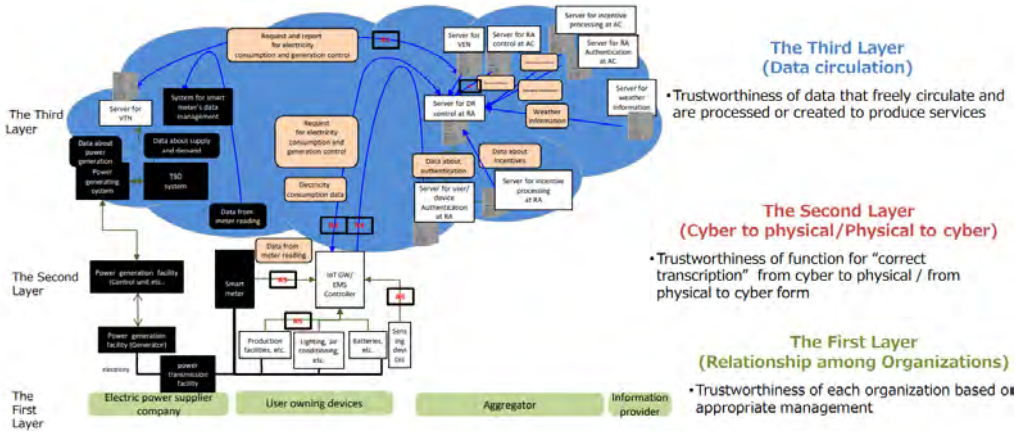
[28] METI, The Cyber/Physical Security Framework.

be confirmed to be trustworthy.

Lastly, the third layer concerns the establishment of trustworthiness in data. Even though trustworthiness of the transcription process from physical space to cyberspace is covered in the second layer, data can be created, edited, processed, and freely exchanged in cyberspace outside of the second layer. Therefore, data integrity is the key element in the third layer, where it forms the basis of trustworthiness for data that are allowed to freely circulate and be processed to produce services.

Referencing this CPSF, the Japanese authorities applied this three-layer security model to the ERAB system. This can be seen in the figure below.

Figure 5.21 Application of the CPSF to the ERAB System – Three-Layer Model



Source: METI.

As such, METI's proposal of the CPSF may serve as a starting point for the creation of a shared basic concept of cybersecurity for distributed energy systems and ERAB systems.

5. Progress of International Standards and References for Cybersecurity

5.1. Development of International Standards by International Standardisation Organisations

Organisational Structure

Cybersecurity efforts at the international level are usually present in the form of industry standards or guidelines. For example, the International Electrotechnical Commission (IEC) developed standards such as the IEC 62443 and IEC TR 63097 for securing distributed energy systems. Other organisations, including the Institute of Electrical and Electronics Engineers (IEEE), also created guidelines to enhance cybersecurity for these systems.

Table 2.24 International Organisations involved in Cybersecurity for DES

Organisation	Organization overview	Activity overview
International Electrotechnical Commission (IEC)	The IEC is a global organization that plays a crucial role in developing and publishing international standards for electrical, electronic, and related technologies.	Its activities related to cybersecurity for distributed energy systems such as Developing the IEC 62443 series for securing Industrial Automation and Control Systems, including distributed energy resources and Creating the **IEC TR 63097** Smart Grid Roadmap for smart grid technology implementation.
Institute of Electrical and Electronics Engineers (IEEE)	The IEEE is a prominent global organization dedicated to advancing technology for the benefit of humanity.	• Developing standards such as IEEE 1547-2018 for DER interconnection and interoperability. • Working on IEEE P2800 standard for securing Inverter-Based Resources (IBRs) interconnected with transmission electric power systems

Source: Created by authors based on IEC and IEEE.

Related Policies and Initiatives

The IEC established a series of cybersecurity standards, especially the IEC 62443 series, titled 'Industrial communication networks – Network and system security' to secure Industrial Automation and Control Systems, which DES would technically fall under. Besides that, there are also other relevant standards and documents, such as the IEC TR 63097 which provides a roadmap for the implementation of smart grid technologies, and IEC 61850 which is applicable for communication protocols and engineering processes for substation automation systems. All relevant standards and documents are summarised in the table below.

In these standards, the IEC establishes several actions as industry best practices or standards, such as the use of multi-factor authentication at key access points to restrict interactions with DES components, application of industry-standard encryption for data transmission and storage (including regular updates for the encryption methods), and the adherence to other sector-specific standards.

Table 2.25 Relevant IEC Standards on Cybersecurity for the Energy Sector

IEC 62443 Series
This comprehensive set of standards is designed to secure Industrial Automation and Control Systems (IACS), including distributed energy resources. It provides a framework for protecting these systems against cyber threats.
Smart Grid Standardisation Roadmap (IEC TR 63097)
This roadmap provides guidelines for selecting appropriate standards and specifications for Smart Energy use cases. It aims to create common guiding principles for end-users and integrators responsible for designing and implementing Smart Energy Systems
IEC 61850
Designed to define data models, communication protocols, and engineering processes for substation automation systems. When applied to DERs, it creates a common framework that allows these resources to interact with the grid and with each other.
IEC 61968-5
This standard defines enterprise interfaces for distributed energy resource management systems (DERMS). It helps in optimising the management of distributed

energy resources
IEC 62351
Developed by Technical Committee 57, provides cybersecurity requirements and guidance for designing security into systems and operations before implementation.

Source: ISA/IEC[29]

Besides the ISA and IEC, there are other international initiatives which may also be relevant to cybersecurity for DES and the energy sector in general. This may be observed in cybersecurity-related initiatives taking place in the European Union (EU), which may also be juxtaposed with those in the United States. These initiatives are summarised in the table below.

Table 2.26 Timeline and Significance of Relevant Initiatives in the EU and the US

Timeline of Events	• 2018: Passing of the EU GDPR • 2019: Passing of the EU Cybersecurity Act • 2020: Signing of the IoT Cybersecurity Improvement Act in the United States • 2022: Passing of the NIS2 Directive & Proposal of the Cyber Resilience Act • 2023: Validation of text of the Cyber Resilience Act • 2024: Formal approval of the Cyber Resilience Act (Tentative)
Significance	Both the NIS2 Directive and the Cyber Resilience Act aim to increase the level of cybersecurity across the EU. • NIS2 Directive: specifies cybersecurity requirements that need to be implemented by EU companies that are considered to be critical infrastructure. o Since NIS2 is a directive, each EU country will have to further define its own cybersecurity laws. In other words, NIS2 specifies the minimum level of cybersecurity to be achieved. o The NIS2 has the potential to become for cybersecurity what the EU GDPR has become for privacy – a worldwide standard that other countries as a best practice for their own legislation

[29] ISA/IEC (n.d.), ISA/IEC 62443 Series of Standards. North Carolina. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards (accessed 26 August 2024).

IEC (2024), Smart Energy Roadmap (based on IEC TR 63097). https://syc-se.iec.ch/iec-63097-smart-energy-roadmap/ (accessed 26 August 2024).

IEC (2024), IEC 61850 Series. Geneva. https://webstore.iec.ch/en/publication/6028 (accessed 26 August 2024).

IEC (2020), IEC 61968-5. Geneva. https://webstore.iec.ch/en/publication/60069 (accessed 26 August 2024).

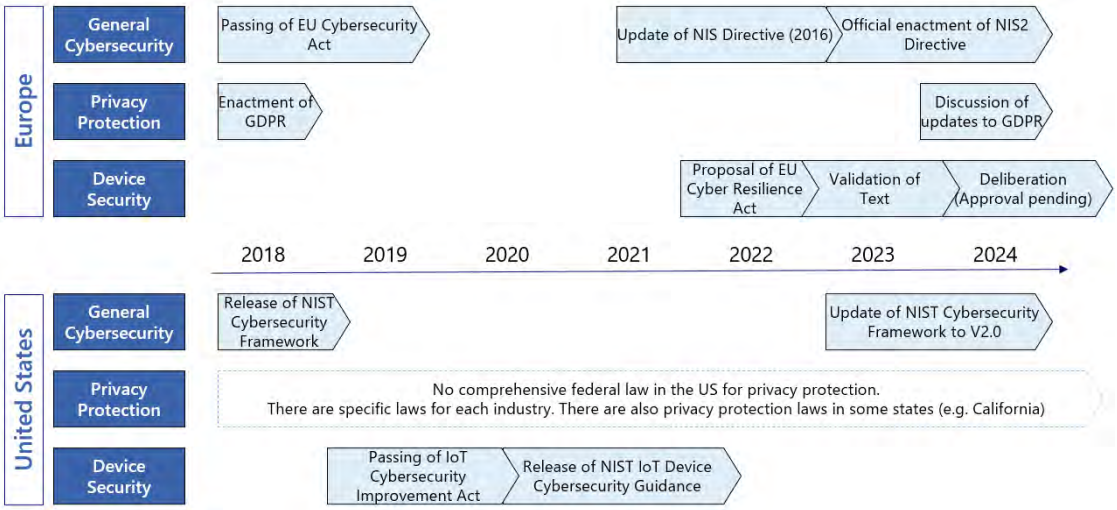
IEC (2024), IEC 62351 Series. Geneva. https://webstore.iec.ch/en/publication/6912 (accessed 26 August 2024).

	• Cyber Resilience Act: establishes a uniform European cybersecurity governance framework to enhance manufacturer responsibility in device security o This Act will mandate compliance measures for manufacturers, requiring that all devices with relevant digital elements must bear an EU mark of conformity o Manufacturers also need to ensure continuous compliance as products undergo updates or modifications o This Act also applies to importers and distributors, who need to ensure that only compliant products enter the EU market

Created by authors based on various sources[30]

These events are shown in a timeline format in the figure below.

Figure 5.22 Timeline of Relevant Initiatives in the EU and the US



Source: Created by authors based on various sources.

[30] GlobalSign (2023), The Cybersecurity Improvement Act 2020 & NIST Cybersecurity For IoT. https://www.globalsign.com/en/blog/cybersecurity-improvement-act-nist-iot (accessed 18 September 2024).

EUR-Lex (2022), Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454 (accessed 18 September 2024).

Tripwire (2024), IoT Security Regulations: A Compliance Checklist – Part 1. https://www.tripwire.com/state-of-security/iot-security-regulations-compliance-checklist-part-1 (accessed 18 September 2024).

Advisera (2024), What is NIS 2 Directive? A detailed and straightforward guide. https://advisera.com/articles/what-is-nis2/ (accessed 18 September 2024).

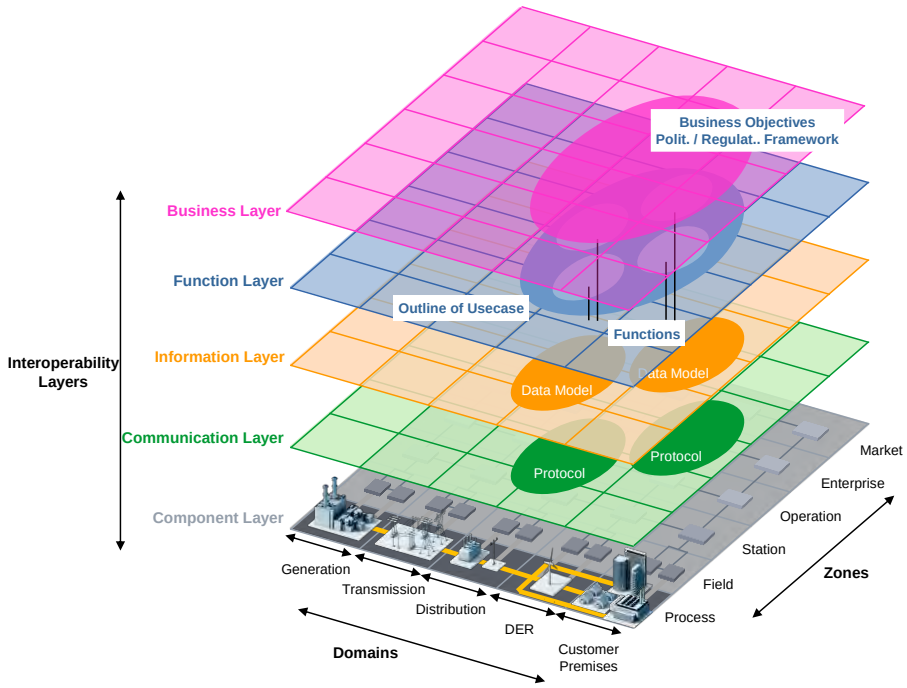
5.2. Framework for Cyber Physical Security

As cyber threats grow more sophisticated and regional or even global in nature, isolated national approaches are no longer sufficient. Therefore, there is a need for a unified framework that would promote collaboration, establish common standards, enable rapid threat intelligence haring, and ensure coordinated responses.

Furthermore, the creation of a framework for cyber physical security will also contribute to the adoption of DERs and ERAB, as market players and other stakeholders will be able to refer to these standards and ensure compliance with them.

Currently, System Committee for Smart Energy (SyC SE) in the International Electrotechnical Commission (IEC) provides systems-level standardisation for smart energy and smart grids. The Smart Grid Architecture Model created by the SyC SE plays the role of being a referable guide for new services running on smart grids.

Figure 5.23 Smart Grid Architecture Model (SGAM) Plane as part of the Smart Grid Standardisation Roadmap on SRD63097



Source: IEC.

In 2022, the SyC SE developed the SRD63443 to be part of the Smart Grid Standardisation Roadmap on SRC63097. This roadmap provides a comprehensive overview of current and emerging standards, placing them in the context of various smart grid applications. Its purpose is to support the selection of appropriate standards for smart grid products, applications, and systems, recognising the complexity and evolving nature of this landscape.

As part of this project, five study groups have been carried out. One of the main goals for these study groups is to establish the foundations that will lead the ASEAN community towards the creation of a unified framework for cyber physical security, starting with its application in the energy sector. At the conclusion of the fifth study group, participants and relevant experts agreed to the shared Basic Concept of Cybersecurity for Distributed Energy Resources, and they also agreed to working together towards the creation of the unified framework. In the future, this unified framework can be pitched as an international standard, possibly to the IEC or another international standardisation organisation.

Chapter 3

Result of the Study Groups

1. Report on the Study Groups

To further our research and promote awareness of DES, ERAB, and related cybersecurity measures, we organised study groups with public utilities stakeholders, academic researchers, and officials from government-linked agencies. There are a total of five study groups held for this project. The aim of these study groups is to arrive at a consensus for a basic concept of cybersecurity for ERAB pertaining to the ASEAN region.

1.1. 1st Study Group

The first study group was held in ERIA's office in Jakarta, Indonesia on 15 October 2024. The main participants for this study group were academic researchers from various universities in Indonesia and Malaysia, public utilities stakeholders, and officials from government-linked agencies. The focus of this study group was three-pronged:

- Introduce the concept of ERAB and the role of aggregators to all participants
- Introduce the importance of cybersecurity for DES and the role of international standards
- Discuss the current state of initiatives regarding ERAB and DES in Japan and several Southeast Asian countries (Indonesia and Malaysia)

This study group featured presentations and comments from various parties as well as an open discussion moderated by Prof. Umejima. There was a wide range of topics covered, including Japan's efforts regarding ERAB and CPSF, growth of the DES market and its feasibility in the ASEAN market, and the importance of establishing a consensus for the formulation of a basic concept for cybersecurity for DES in the ASEAN market.

Table 1 Presentations, Comments, and Open Discussion for the 1st Study Group

Speaker, Designation, Organisation	Content of Presentation/ Comment/ Open Discussion
Dr Nuki Agya Utama, Head of the Asia Zero Emission Center (AZE Center), ERIA	Welcome address • AZEC joint statements and activities • ERIA's mission • Role of the AZE Center • Importance of cybersecurity for DES and smart grids in ASEAN • Purpose of the 1st Study Group
Dr Masaki Umejima, Convener of the Smart Energy Development Plan, System Committee, International Electrotechnical Commission, Keio University Cyber Civilisation Research Center & IEC	Keynote address • Introduction of 2 new terms – ERAB and CPSF • Role of cybersecurity – not just technological, but also economic and political • Introduction of IEC System Committee Smart Energy (SyC SE) • Role of IEC in defining ERAB as an international standard
Mr Akinori Kahata, Deputy Director, Electricity Industry and Market Office, Agency for Natural Resources and Energy, METI	Presentation: Japan's initiative for ERAB and CPSF • Current situation of energy use and decarbonisation in ASEAN • Introduction of AZEC concept and initiatives • Introduction of the role of the aggregator and related businesses (demand response and regional microgrids) • Introduction of the license for aggregators under the Electric Business Act • Introduction of CPSF and related cybersecurity initiatives (e.g. JC-STAR) • Expectations from the Japanese government regarding aggregators
Mr Katsuya Tokuda, Manager, NRI Singapore	Presentation: Future potential of cybersecurity for DES and ERAB in ASEAN • Growth of the DES market and the use of DES and ERAB to provide balancing power, renewable energy, energy savings, and sustainable power supply • Feasibility of DES • Cybersecurity trends in various countries around the world
Ms. Supanuch (Yukyik) Pongthanacharoenkul, Secretary in charge of Community Building in	Presentation: Collaboration between ASEAN and Japan to address ERAB and CPSF

Thailand, Keio University Global Research Institute (KGRI)	• Current situation of Japan's competitiveness vis-à-vis ASEAN countries (Thailand, Malaysia, and Indonesia) • Challenges faced thus far • Purpose of the CCRC's research project
Dr Selvakumar Manickam, Associate Professor, National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM)	Comment: Current situation of the Cybersecurity Research Center in USM regarding ERAB and DES • Current focus on manufacturing, due to the location of USM in the north of Malaysia • Potential applicability of security elements for manufacturing (CPSF) for the energy sector • Need to narrow the scope to consider implementation case studies in Malaysia in 2025
Dr Chaodit Aswakul, Head of Electrical Engineering Department, Chulalongkorn University	Comment: Current situation of the Chulalongkorn University Electrical Engineering Department (CUEE) regarding ERAB and DES • Creation of the RE100 Community Microgrid, R&D Playground, and Living Lab @ Gewertz Square • Current situation of the microgrid (PoC) • Explanation of cybersecurity techniques employed for the microgrid • Collaboration with the Center of Excellence in Electrical Power Technology (CEPT)
Mr Suharto, Expert Staff in Technology and Transportation Energy to The Minister of Transportation, Ministry of Transporatation	Closing address • Importance of addressing critical issues such as technology, energy, and cybersecurity in an increasingly interconnected world • Necessity to update relevant guidelines and frameworks to make ERAB a reality • Importance of ERAB and DES to ASEAN to modernise grids and decarbonise • Key success factors for ERAB – technological advancement and the establishment of trust in DES through proper frameworks and commitment from various stakeholders
Open discussion	
Dr Mochamad Teguh Kurniawan, Head of Computer Network and Operation System Laboratory, Telkom University	• What is the current progress of development and implementation of ERAB in Japan?

Akinori Kahata, METI	• History of ERAB can be traced back to the consideration of demand response after the Fukushima nuclear disaster • From 2012–2013, Japan started to push for HEMS and BEMS to manage energy demand. As a continuation of that, from 2015 onwards, Japan created the concept of ERAB • Japanese government has the capabilities and the willingness to provide support for interested parties to join in this market
Dr Selvakumar Manickam, USM	• Key point to note when moving from planning to implementation is identifying and delineating between ideal/ goals and real-world achievable targets • Importance of balancing several tenets – openness, trust, and security • Importance of collaboration between different sectors – government, industry, and academia • Timeframe for implementation should not take more than a year, because of the rate of changes in the cyber world
Mr Harris, Head of The Center for Survey and Testing Electricity, Balai Besar Survei dan Pengujian KEBTKE, Ministry of Energy and Mineral Resource (ESDM)	• There are already rules in Indonesia to introduce new facilities or technologies to increase energy efficiency • Requirements of more support for industry stakeholders to hold demonstration projects and provide subsidies for companies which are considering entering into this market • Example of Kyudenko's use of control systems to convert solar energy to electricity in Kalimantan • Key issue is to consider the issue of long-term business feasibility for the operators, after government subsidies have ended
Mr Katsuya Tokuda, NRI Singapore	• Problems faced by Kyudenko in Kalimantan (business feasibility and profitability in the long run due to maintenance and operation costs for facilities that are spread out across many islands; battery storage systems which run on diesel are used, and they may run against the goal of carbon neutrality)
Dr Chaodit Aswakul, Chulalongkorn University	• Current systems for the microgrid are still at the testbed stage and not yet ready for implementation

	• Expressed interest to get involved in the testing phase during the creation of new guidelines (learning by doing)
Dr Masaki Umejima, Keio University	• Importance of addressing and using international standards, as pilot studies based on them will allow operators to track and benchmark data against other stakeholders in other countries • Reiteration of the goals of the 1st study group – to introduce the high-level guidelines and framework (CPSF). Future study groups will deep-dive into them • Frameworks such as CPSF and NIST will apply across countries as guidance materials, however guidelines such as the ERAB Security Guidelines in Japan should be created by each government (with coordination by ERIA). At the same time, the various universities will play the role of publishing academic reports which cover the necessary measures for cybersecurity (e.g. USM will publish a piece for the Malaysian context) • At the implementation stage, efforts should be from a combination of industry, government, and academia
Mr Gunawan Witjaksono, President, Cyber University	• The 1st study group has not touched a lot about CPSF. What about the coverage of cyber systems?

Working towards the next study group, the attendees agreed to the establishment of a tight-knit community. All attendees agreed to the mutual sharing of materials and information. Furthermore, to facilitate closer communication, a WhatsApp group chat was created to include all high-level attendees.

At the end of the 1st study group, the attendees discussed the potential date and venue for the 2nd study group. Dr Selvakumar of USM mentioned that his laboratory would be able to host the 2nd study group, and Dr Umejima mentioned that the CCRC secretary would support him in terms of organisation and logistical planning.

Figure 6.1 Pictures of the 1st Study Group

1.2. 2nd Study Group

The second study group was held in virtually on 20 January 2025, with over 50 participants from Malaysia, Indonesia, Thailand, and Japan. Hosted by IPv6 Forum Malaysia and ERIA and endorsed by the Cyber Civilisation Research Center (CCRC) at Keio University, Japan, this study group aimed to explore the growing importance of cybersecurity in Distributed Energy Systems (DES) and their integration with IoT technologies.

This study group provided a platform for experts, policymakers, and researchers to discuss the evolving challenges and opportunities in securing cyber and physical systems in electricity sector. As DES continue to grow in importance across ASEAN, the discussions focused on the need for standardised cybersecurity frameworks, sharing of best practices, and strengthening cross-border and international cooperation.

The key topics discussed include:

- Strengthening cyber and physical security frameworks (CPSF) for energy IoT systems
- Standardisation efforts for cybersecurity regulations in distributed energy systems (DES)
- Development of testbeds and regional cooperation for cybersecurity solutions
- Establishing long-term strategies to secure ERABs across ASEAN nations

Table 3.2 Presentations, Comments, and Open Discussion for the 2nd Study Group

Content of Presentation
Cybersecurity in Energy Systems • As a moderator, Dr Masaki Umejima, highlighted the importance of establishing international standards for Distributed Energy Systems (DES), including data interfaces and security protocols.
CPSF Framework Overview • The Cyber-Physical Security Framework (CPSF) was introduced, emphasising the need for security at three layers: cyber space, cyber-physical space, and existing standards. The six essential elements of CPSF were outlined: o Organisations: Identifying trusted organisations o People: Considering human behaviour and perspectives in cybersecurity o Components: Ensuring security in hardware and software o Data: Managing data privacy and protection, especially in AI-driven systems o Procedure: Developing guidelines to enhance trust and security o System: Understanding how these elements work together
Recommendations and Testbeds • The workshop proposed the creation of testbeds in ASEAN countries to evaluate cybersecurity risks in DES and energy systems, exchange findings, and foster research collaboration.
International Standards and Data Security • There was a discussion on balancing national security with international cybersecurity standards. It was emphasised that while data is managed within each country, international standards could be adopted for technical components, encryption, and authentication procedures.

AI and Data Complexity

- As energy systems evolve, the integration of AI and automated data generation was noted as a major challenge for cybersecurity. Participants emphasised the importance of new strategies and understanding the increasingly complex data structures that these systems generate.

Existing Standards and Updates

- Experts noted the need for continuous updates to existing standards like NERC CIP, particularly as cybersecurity threats evolve. Participants agreed that while standards are essential, they must be flexible and regularly updated to adapt to new technological advancements.

At the end of the 2nd study group, the attendees scheduled another meeting for February or March 2025. The following meeting will focus on creating a common understanding of cyber-physical security systems, tailored to each country's policies and requirements, enhancing knowledge exchange on the research efforts related to ERAB and the CPSF, as well as collaborating on publishing white papers with cybersecurity recommendations for energy systems in the ASEAN region.

It was agreed that in the next meeting, participants will present their research proposals, progress updates, and further advancements in the integration of cybersecurity and IoT in the energy sector.

Figure 6.2 Collage of Participants of the 2nd Study Group

*Note: Not all participants are depicted in this collage.

1.2.1. 3rd Study Group

The third study group, 'Cybersecurity for Energy & IoT ERIA ERAB & CPSF Workshop 2025', was held on 22 January 2025 at Hotel Maya, Kuala Lumpur, Malaysia. The event was hosted by IPv6 Forum Malaysia and endorsed by the Economic Research Institute for ASEAN and East Asia (ERIA) and the Cyber Civilisation Research Center (CCRC) at Keio University, Japan. The study group marked a significant milestone in fostering international cooperation on energy resource security and IoT cybersecurity, providing a

platform for knowledge exchange and expert collaboration across ASEAN nations.

The hybrid event featured 40 in-person experts and over 50 online participants, including professionals from Malaysia, Japan, Indonesia, Thailand, and other ASEAN countries. Those unable to attend physically joined via video conferencing (conference link: https://clitehd.com/erabworkshop).

The key focus areas included:

- Strengthening cyber and physical security frameworks (CPSF) for IoT devices in the energy sector
- Facilitating cross-border collaboration amongst ASEAN cybersecurity and energy experts
- Discussing standardisation efforts for cybersecurity regulations and energy IoT integration
- Establishing long-term cooperation for securing distributed energy resource aggregation businesses (ERABs)

Table 3.3 Presentations, Comments, and Open Discussion for the 3rd Study Group

Speaker, Designation, Organisation	Content of Presentation/ Comment/ Open Discussion
Prof. Emeritus Dr Sureswaran Ramadass, Chairman – IPv6 Forum Malaysia, Chairman, APAC IPv6 Council, Subject Matter Expert, Malaysian Communications and Multimedia Commission (MCMC)	Welcome address • Introduction of ERAB, CPSF, ERIA, CCRC • Introduction of IPv6 Forum Malaysia and its important role in securing energy systems in Malaysia through research centre, workshops, and Smart Home IoT Security certification programme
Mr Naoto Okura, Director General for Research and Policy Design – Economic Research Institute for ASEAN and East Asia (ERIA)	Welcome address • Mission: Conducts impactful research and policy recommendations to advance economic integration in East Asia, especially ASEAN, focusing on decarbonisation roadmaps, market enablers, and sector-specific actions • Cybersecurity & Energy Sector Goals (supported by METI, CCRC, and NRI Singapore): Assess the status of DES adoption and cyber-physical security in the energy sector • Strategic Actions: Develop DES cybersecurity guidelines, creates feasible action plans including testbeds, and facilitate a secure and decarbonised energy future
Prof. Karen Morgan, President – RUMC (RCSI & UCD Malaysia Campus)	Keynote address • Similarities between medical and energy IoT security, emphasis on the need for robust data protection and system resilience

	• Data privacy risks, regulatory compliance, and cybersecurity threats in both healthcare and energy sectors • Fostering multidisciplinary innovation, encouraging collaborative research and cross-industry partnerships to drive impactful solutions from these workshops and the upcoming activities
Prof. Ir. Dr Khairul Salleh Bin Mohamed Sahari, Vice Chancellor – Universiti Tenaga Nasional (UNITEN)	Keynote address • Introduction of UNITEN, its mission, and the impressive achievement including 97.3% employability rate in cybersecurity graduates • Introduction of 6 research institutes including power engineering, sustainable energy, policy research, energy infrastructure Informatics and computing in energy, and nuclear energy • Introduction of the case of Cyberjaya Green Tech Industrial Park • Call for collaboration in embracing the adoption of IPv6 to enhance energy security and explore the synergy between technology and energy management for a sustainable future
Dr Masaki Umejima, Convener of the Smart Energy Development Plan, System Committee, International Electrotechnical Commission, Keio University Cyber Civilisation Research Center & IEC	Keynote address • Cyber-physical integration for secure energy management and IoT • Position of ERAB within electricity system • IEC SRD63443, ISO/IEC 14543-4-3 (ECHONET Lite) as an open standard to DERs at customer premise • Not only ECHONET Lite, but there are also other communication protocols like Matter (Europe), and NIST (US) • CPSF highlights six elements (Organisation, people, component, data, procedure, system) and three layers (Data, IoT, relationship amongst organisations) to ensure trust and interoperability • Five suggestions for enabling CPSF and ERAB o Develop a community o Create common understanding about CPSF and ERAB with common criteria ISO/IEC15408 o Empower practical studies about CPSF and ERAB such as testbed in USM o Educate engineers implementing CPSF and ERAB through Smart Home and CPSF-ERAB Security Certification o Publish research outcomes of CPSF and ERAB: ERIA white paper spotlighting energy IoT and DERs
Assoc Prof. Dr Shankar Karuppayah, Deputy Director – Cyber Security Research Centre (CYRES), University Sains Malaysia	Keynote address • Critical role of energy systems in national security and economic resilience.

	• Global cyber threats: Discussed major incidents like Stuxnet (Iran), malware-induced blackouts (Ukraine), and ongoing cyberattacks on Romania's electricity grid. • Challenges in Malaysia's energy sector: Highlighted human factors, system complexity, and the need to prioritise cybersecurity for national energy resilience. • Introduction of BitRanger and Ownsight: low-cost, certified solutions for threat monitoring, penetration testing, and vulnerability assessment, aligned with ECHONET and international standards
Mr Patrick Veron, SFC Forum Foundation, Japan & Ir. Ts. Mahesvaran Sibeperegasam, Lead (Emerging Solution), TNBX, Tenega National Berhad	Keynote address • Introduction of ERAB in empowering Malaysia's Green Energy Aspirations • Overview of Malaysia's National Energy Transition Roadmap, its challenges, the needs of energy flexibility • VPP and demand response are one of beneficial solutions for balancing demand and supply • Introduction of ERAB, its stakeholders, ERAB applications, ERAB value chain, timeline from February 2025 • Potential business models and strategies to implement ERAB in Malaysia including: o Management of air conditioners o EV and batteries management
Mr Teguh Prasetya, Chairman – Indonesia Internet of Things Association (ASIOTI)	Presentation • Overview of technology singularity, IoT adoption, security challenges, regulatory frameworks, and the main common IoT Security architectures in Indonesia • Growing role of embedded AI in creating people-centric digital solutions for industry and manufacturing • Future-proofing security: Collaboration and innovative infrastructure are key to addressing shorter technology lifecycles and managing IoT security to overcome challenges such as network security, data & platform security, device & application security
Assoc. Prof. Wanchalerm Pora, Department of Electrical Engineering, Faculty of Engineering, Chulalongkorn University, Thailand	Presentation • Cybersecurity design of Grid Edge Network for Gewertz Square • Home-grown Smart Devices including grid-forming inverter, DynaWatch (IEEE c37.118.2), smart meter/switch (ECHONET Lite), and EMS • Key security design idea of RE100 Grid Edge consists of physical security, device security, operational security, data security, and standard compliance

Dr Ary Setijadi Prihatmanto, S.T., M.T., Center for Excellence for Defense and Security Science and Technology of Bandung Institute of Technology, Indonesia	Presentation • Industry 4.0 & Digital Economy: Advancing cyber-physical systems for industrial automation and economic growth • CPSF in Indonesia: Addressing IoT trustworthiness, cybersecurity risks, and regulatory challenges • Ecosystem & Digital Transformation for community 21: Collaboration amongst tech firms, academia, and policymakers to drive education 21, smart cities, automation, defence and security, etc.
Open discussion: Cybersecurity for Energy & IoT (Policy and Regulations)	
Dr Navaneethan C. Arjuman Senior Lecturer – Multimedia University	Questions: • What are the biggest cybersecurity challenges currently facing the energy sector in relation to IoT adoption? • Are existing cybersecurity regulations and standards for IoT devices sufficient to address the evolving threats in the energy sectors • With IoT devices generating vast amounts of data, how can organisations ensure compliance with data privacy regulations like GDPR or similar laws in other regions? • How can IPv6 adoption help improve security for IoT devices in the energy domain, and what are the associated risks? • What is the role of global cooperation in securing IoT networks for interconnected energy grids?
Assoc Prof. Dr Shankar Karuppayah Deputy Director - Cyber Security Research Centre (CYRES), University Sains Malaysia	Comment • The policies should enforce the co-existence of legacy devices and new technologies • Security assessment frameworks and real-time threat detection are essential for safeguarding critical energy infrastructure • Energy management systems have long been in place, but varied infrastructures and policies across countries create security challenges • Standardised regulations must evolve to ensure resilience, interoperability, and long-term system security
Mr Hiroshige Muraoka, President, Nomura Research Institute Singapore	Comment • Smart grid systems will be developed in line with each country's energy strategies while ensuring interoperability • METI, CCRC, and NRI will release the revised draft of the ERAB Cyber Security Guidelines in March 2025, addressing emerging cyber threats in energy systems • Cyberattacks on the energy sector are rising, but Cyber and Physical security regulations vary across

	countries, reflecting different policy priorities and approaches
Prof. Masaki Umejima Convener of Development Plan – IEC System Committee Smart Energy, Japan	Comment • New cyber physical security standards are essential • Given the complexity of electricity systems, comprehensive guidelines are impractical. A risk-based approach is recommended, including: o Security assessments (e.g. IEC or other relevant international standards) to identify specific risks o Development of technical countermeasures (e.g. CPSF) o Self-assessments and government-driven assessments • As attack detection is the most challenging aspect, CPSF design should prioritise robust attack detection capabilities
Mr Shaifubahrim Bin Mohd Saleh Director, Cybersecurity Malaysia	Comment • Top five global risks (World Economic Forum): Mis/disinformation, extreme weather events, state-based armed conflict, societal polarisation, cyber espionage and warfare • Human factor is the key to most cyber incidents • Culture and society shape human behaviours and cyber securities practices • Continuous education is critical for maintaining awareness and preparedness in the face of evolving threats
Closing address	
Mr Akinori Kahata, Deputy Director Electricity Industry and Market Office, Agency for Natural Resource and Energy, Ministry of Economy, Trade and Industry (METI), Japan	Closing address • AZEC-ERAB: Action plan for electricity system reform (decarbonisation, decentralisation, digitalisation) • Aggregator is a key player to promote DES and Demand Response (DR) • CPSF is the minimum cybersecurity requirements for ERAB • Japan Cyber STAR (JC-STAR) secures IoT products to launch in March 2025

Figure 6.3 Pictures of the 3rd Study Group

1.4. 4th Study Group

The fourth study group was held online via Zoom on 5 March 2025, with 21 participants from Malaysia, Japan, Indonesia, and Thailand. The event was hosted by ERIA and endorsed by NRI and CCRC at Keio University. The study group fostered a common understanding of cyber-physical security and provided a platform for knowledge exchange and expert collaboration across ASEAN nations.

The discussions were focused on the security triangle of ERAB and CPSF, covering three layers (cyberspace, physical space, and their connections) and six key elements (organisation, people, components, data, procedures, and systems). The workshop also explored risk assessment case studies from Malaysia and Japan, emphasising the

importance of trust in data exchange between organisations and devices. Participants highlighted the need for proactive security measures and a unified approach to cyber-physical systems security across Asia. Future workshops and testbeds were also discussed.

Table 3.4 Key Discussion Points and Findings of the 4th Study Group

Key Topic	Content
Cyber Physical Security Framework (CPSF)	• Establishing a common understanding of cyber-physical security frameworks • Managing data flow between physical and cyber spaces • Secure data exchange standards between organisations • Security considerations for three layers: physical space, cyberspace, and their connection • Emphasis on CPSF's six key elements: Organisation, People, Components, Data, Procedures, and Systems
Proactive Risk Evaluation and Management	• Identifying and mitigating risks before breaches occur • Lessons from industry 4.0, manufacturing and energy sectors • The importance of proactive rather than reactive security responses • Addressing cyber threats in closed systems
Trust Establishment in Data Exchange	• Ensuring organisation-to-organisation trust before enabling device-to-device and data-to-data trust • Translating physical events into secure digital data • Addressing risks like spoofing attacks, with measures such as authentication, encryption, and access control
Security in Cyber-Physical Systems and Energy IoT	• Three layers of trust: Organisation-to-Organisation, Device-to-Device, Data-to-Data

	• Importance of device authentication and network access rights • Addressing human and organisational factors, which cause 70% of vulnerabilities • Key security measures: asset management, risk assessment, and supply chain risk management
International Collaboration on Cyber and Physical Security	• Developing a shared understanding of cyber-physical security across Asia • Presentation of 58 attack scenarios from NRI's security assessments (subject to local context and regional variations) • Need for attack tree analysis to map risks and countermeasures • Importance of sharing cyber-physical attack scenarios and mitigation strategies • Consideration of hardware vulnerabilities alongside software security

Working towards the fifth study group in Bandung, Indonesia, the participants agreed on the following action items and steps to be taken next, which are summarised in the following table.

Table 3.5 Action Items and Next Steps raised in the 4th Study Group

Action Item	Next Step
Standardisation Efforts	• Develop a common cybersecurity standard for ERAB and DES across ASEAN, considering local contexts • Enhance collaboration on cyber physical security frameworks
Risk Assessment & Mitigation	• Implement international standards such ISO/IEC 31000 for risk evaluation • Define attack scenarios and countermeasures
Workshop & Research Expansion	• Strengthen collaboration with ERIA, academia, government, state-owned agencies, and industry • Enhance international cybersecurity knowledge sharing

1.5. 5th Study Group

The fifth and final study group was held in person in Hotel Savoy Homann Bandung, Indonesia on 24 April 2025, with more than 50 participants from Indonesia, Thailand, Malaysia, Singapore, and Japan. The event was hosted by ERIA and endorsed by NRI and CCRC at Keio University. The study group was the culmination of the four previous study groups, where participants discussed the contextualisation and application of the CPSF to their own countries, agreed to the common understanding (shared concept) of cyber-physical security, and called for ASEAN-wide collaboration efforts.

Participants shared their understanding and application of the CPSF in each of their countries, covering key concepts such as the security triangle of ERAB and CPSF as well as the three layers of cyberspace, physical space, and their connections, and the six key elements (organisation, people, components, data, procedures, and systems). The study group also included presentations from grid operators and academic researchers, who shared their findings on the current state of DERs in each ASEAN country.

Participants also highlighted the need for a shared common understanding regarding cyber-physical systems (especially related to the energy sector), as well as the importance of formulating a set of standards that is flexible enough to be applied across the ASEAN countries (taking into account each country's context) and also robust enough to be applied on the international stage as an international standard.

Table 3.6 Presentations and Keynote Speeches for the 5th Study Group Plenary Session

Speaker, Designation, Organisation	Content of Presentation/ Keynote Speeches
Mr Shinichi Kihara, Director-General for Energy and Environmental Policy, Ministry of Economy, Trade and Industry, Japan	Opening remarks • Introduction of the AZEC Initiative and AZEC Power Initiative • Actions to promote liberalisation of electricity grids, green initiatives and decarbonisation, sustainable fuels, and next-generation industries • Desires for the Study Group, regarding knowledge sharing and plans for the future
Dr Nuki Agya Utama, Head of the Asia Zero Emission Center (AZE Center), ERIA	Welcome speech • Introduction of ERIA and its vision • Current status of DES across the ASEAN region • Raising awareness and building collaboration regarding CPSF and ERAB • Exploration of DER strategies and development of robust security frameworks • Addressing emerging vulnerabilities, threats, and countermeasures in energy infrastructure • Future goals of the ASEAN Power Grid
Prof. Ir. Purnomo Yusgiantoro, Special Advisor to the Indonesian President for Energy	Opening remarks • Intersection of energy, technology, and security • Growing energy demand in Asia • Regional commitments by ASEAN and AZEC • Indonesia's role in ASEAN's energy transition • Securing energy in the digital era (cyber-physical threats, ERAB, and global standards)
R. Tjahjo Khurniawan, Head of National Cyber and Crypto Agency (BSSN), represented by Deputy of Strategy and Policy of Cyber Security and Cryptography, Air Vice Marshal	Keynote speech • Total traffic anomaly activities for the energy sector in Indonesia • Cybersecurity legislative frameworks in Indonesia • National Cyber Security Strategy (NCSS) of Indonesia and key strategic efforts to strengthen national cybersecurity • Interdependencies of the CII sectors • Quadruple helix collaboration in cybersecurity (government, academia, industry, and community)
Dr Jun Murai, Senior Advanced Research Project Professor, Keio University, Japan, Advisor to the Digital Agency, Japan, Special	Keynote speech • Definition of digital infrastructure • Introduction of the Space Integrated Computing Network

Advisor to the Japanese Cabinet	• Cybersecurity perspective of PNT – positioning, navigation, and timing • Japan's latest efforts for cybersecurity
Dr Masaki Umejima, International Electrotechnical Commission System Committee Convener of the Smart Energy Development Plan	Keynote speech • ERAB with CPSF and trusted design for cyber and physical systems • How to balance electricity supply and demand • Use of open standards for DERs at customer premises • Recommendations for ERAB security, as part of cyber physical security • Cybersecurity guidelines of ERAB version 2.0
Dr Soontorn Sirapaisan, Acting Head of Research and Research Collaboration Section, National Cyber Security Agency (NCSA) Thailand	Keynote speech • History and role of the National Cyber Security Agency (NCSA) of Thailand • Energy statistics of Thailand • Ministry of Energy's National Strategy and Master Plan • Future Power Grid in Thailand • Provincial Electrical Authority (PEA) and Metropolitan Electricity Authority (MEA) efforts
Dr Haryanto, Minister of Energy and Mineral Resource of Republic of Indonesia, represented by Head of Planning Bureau	Keynote speech • Indonesia's oil production • Strategic initiative and strategic investment downstreaming roadmap in Indonesia • Regulations related to energy conservation, business, and management in Indonesia • Decarbonisation programmes • Current situation of security measures for the energy sector
Mr Akinori Kahata, Ministry of Economy, Trade and Industry, Japan, Deputy Director, Agency for Natural Resources and Energy	Keynote speech • Importance of DES for GX and carbon neutrality • Japanese outlook for energy supply and demand in FY2040 • Structural changes in the electricity system towards carbon neutrality • Japanese activities in the promotion of ERAB, demonstration projects for ERAB, and creation of cybersecurity guidelines for ERAB • Global South Future-Oriented Co-Creation Project
Mr Abdan Hanif Satria, Director of Corporate Planning and Business Development at PT. PLN (Persero), represented by	Keynote speech • Introduction of PLN and the Green Enabling Super Grid

Executive Vice President of Corporate Business Development and Investment Division	• Evolution of the energy system from a one-way fossil-based grid to a smart multi-directional network based on distributed generation • Role of aggregators • Issues faced in Indonesia's transition to ERAB • PLN's Smart Grid Initiative
Dr Ary Setijadi Prihatmanto, Bandung Institute of Technology, Head of the Center for Excellence in Defense and Security Science and Technology	Keynote speech • Introduction of smart systems and the integration of 4 technologies – IoT & robotics, human-content interaction, modelling, simulation & artificial intelligence • Requirements for the implementation of CPSF standards and challenges faced • Importance of security in smart systems and the People, Process, Technology (PPT) framework • Proposed Programme for Strategic Framework for Smart Energy
Dr Manickam Selvakumar, Head of Cyber Security Research Center, University Sains Malaysia (USM)	Keynote speech • History and introduction of USM • Potential of ERAB and its current status in Malaysia • Role of cyber-physical systems in ERAB and DER • Malaysian context for DER security recommendations and application of CPSF in Malaysia • ECHONET Lite Security Assessment in Malaysia
Mr Hiroshige Muraoka, President, Nomura Research Institute Singapore	Keynote speech • Economic growth in Southeast Asia and the role of distributed energy systems in ASEAN • Introduction of DERMS initiatives in ASEAN • Each ASEAN country's smart grid/DES strategy • Level of ERAB readiness in ASEAN

Table 3.7 Presentations in Breakout Room 1 of the 5th Study Group – Focus on CPSF

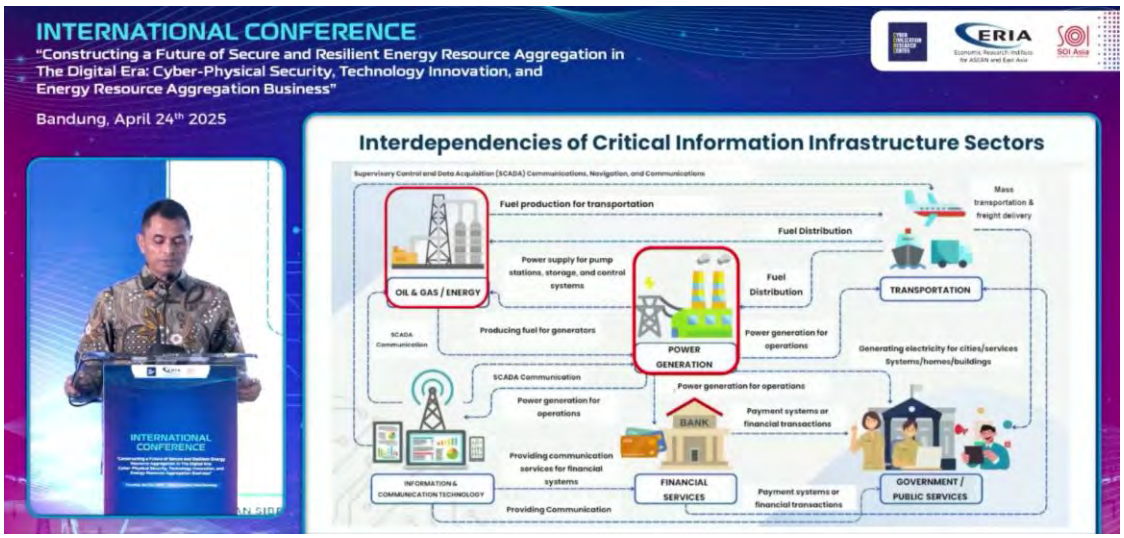
Speaker, Designation, Organisation	Content of Presentation
Dr Andhika Prastawa, Coordinator of Smart Electrical Systems Research Center for Energy Conversion and Conservation, Energy and Manufacturing Research Organisation, The National Research and Innovation Agency (BRIN)	Presentation • Development of Physical Cyber Security Technologies for Energy Infrastructure

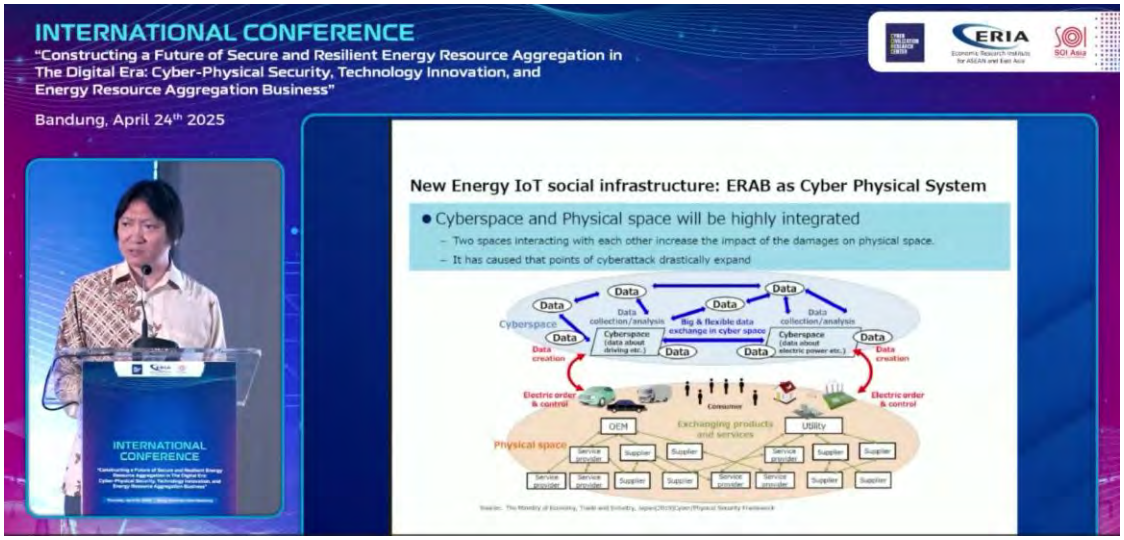
Mr Wahyu Ahadi, PT. PLN (Persero), EVP STI (Executive Vice President Information and Technology System)	Presentation • Application of CPSF in electricity Infrastructure
Mr Alfan Prasekal, S.T., M.Sc. (DIC)	Presentation • Application of Machine Learning and AI in Detecting Cyber Threats to Energy Infrastructure
Mr Jitsatha Thatavakorn, Director, Digital Technology Operation Division, Electricity Generating Authority of Thailand (EGAT)	Presentation • Cyber-Physical Security in the Smart Grid to Enable a Trusted Energy Transition
Dr Basuki Suhardiman, Bandung Institute of Technology & Dr Masaki Umejima, CCRC, Keio University	Presentation • Trust in energy IoT with the open network policy from the history of internet penetration

Table 3.8 Presentations in Breakout Room 2 of the 5th Study Group – Focus on ERAB

Speaker, Designation, Organisation	Content of Presentation
Prof. Goi. Hoe Chin, NUCB Business School	Presentation • Startup Pathway for Integration of Cyber-physical Systems Security with Energy Resource Aggregation Business Sector in Singapore
Mr Takahiro Endo, Producer, Business Innovation Dept. Business Innovation Unit, INTEC Inc.	Presentation • 'UCHITAS' Platform for ERAB
Mr Norio Shigetomi, Chief Representative, Kyudenko Indonesia Representative Office	Presentation • Introduction of micro grid development in remote islands
Mr Patrick Veron, Executive Director, EWIS Asia	Presentation • Deep Dive into Malaysia's Energy Policy 2050 and Current ERAB Efforts
Mr Sarawut Phoolma, Chief of System Operation Department, Power System Control and Operation Division, Electricity Generating Authority of Thailand (EGAT)	Presentation • Grid System Operator in Thailand

Figure 6.4 Pictures of the 5th Study Group




INTERNATIONAL CONFERENCE
"Constructing a Future of Secure and Resilient Energy Resource Aggregation in The Digital Era: Cyber-Physical Security, Technology Innovation, and Energy Resource Aggregation Business"
Bandung, April 24th 2025
ERIA
INTERNATIONAL CONFERENCE
New Energy IoT social infrastructure: ERAB as Cyber Physical System
Cyberspace and Physical space will be highly integrated
Two spaces interacting with each other increase the impact of the damages on physical space.
It has caused that points of cyberattack drastically expand
Data
Cyberspace
Physical space
Data collection/analysis
Big & flexible data exchange in cyber space
Data creation
Electric order & control
Consumer
Exchanging products and services
OEM
Utility
Supplier
Service provider


"Constructing a Future of Secure and Resilient Energy Resource
The Digital Era: Cyber-Physical Security, Technology Innova
Energy Resource Aggregation Business"
Thursday, April 24, 2025 | Savoy Homman Hotel Bandung


Energy Resource Aggregation Business
Thursday, April 24, 2025 | Savoy Homman Hotel Bandung

2. Key findings from the Study Groups

The findings from the five study groups highlight the transformative potential of DERs in advancing decarbonisation while emphasising the importance of regulatory support, industry collaboration, and cybersecurity preparedness. As ASEAN countries move towards a decentralised, low-carbon energy future, policymakers, aggregators, and industry leaders must work together to address integration challenges, promote market participation, and safeguard energy infrastructure from cyber threats. The success of this transition will depend on continuous innovation, proactive governance, and international cooperation to ensure a secure, sustainable, and efficient energy landscape.

2.1. Future of Distributed Energy Resources in the Decarbonisation Journey

The transition towards decarbonisation is driving the increased adoption of distributed energy resources (DERs) as a critical component of sustainable energy systems. As nations strive to achieve zero carbon emissions, DERs – comprising solar photovoltaics, wind power, battery storage, and demand response systems – are expected to play an essential role in enhancing grid flexibility and reducing dependency on fossil fuels. The shift towards DERs is projected to accelerate, particularly in the ASEAN region, where energy demand continues to grow. The integration of these decentralised systems will support energy security, cost reduction, and a more resilient power supply while aligning with international climate goals.

However, the widespread deployment of DERs presents new challenges. The increased penetration of variable renewable energy sources requires advanced energy management solutions and regulatory frameworks that ensure seamless grid integration. Additionally, the transition necessitates the development of clear market structures that promote investment in DER technologies while ensuring fair competition and reliability.

2.2. Value of Aggregation in the Future of the Grid

As seen in the case study of Japan, aggregation is emerging as an important concept in the overall energy landscape. The ability to manage and optimise multiple distributed energy resources (DERs) under a single framework presents a valuable opportunity for improving grid efficiency and facilitating participation in energy markets, demand response programmes, and grid balancing services. Industry stakeholders, including both new market entrants and established power companies, are increasingly exploring aggregation as a means to enhance their role in the energy transition. By consolidating energy from various sources, aggregation has the potential to improve the coordination of decentralised energy systems, contributing to overall system stability and flexibility.

Beyond technical coordination, aggregation is also becoming a key enabler of broader energy market developments. It offers a pathway for regulatory alignment, new business model exploration, and expanded market access for DER owners. Across the ASEAN region, interest in aggregation is growing as countries seek to balance economic growth, environmental sustainability, and energy security. As this concept gains traction, governments and regulatory bodies have an opportunity to shape policies and frameworks that support the effective integration of aggregation within the broader energy system. Encouraging discussions on licensing structures, operational standards, and market incentives will be crucial in ensuring that aggregation contributes meaningfully to a more resilient and dynamic energy ecosystem.

2.3. Cooperation between Government, Academia, and Industry

Taking reference from keynote addresses and presentations at the Study Groups[31], achieving a decarbonised energy future requires a concerted effort from government institutions, academic researchers, and industry stakeholders. These three sectors must collaborate to develop innovative policies, technological advancements, and market mechanisms that promote DER adoption.

1. Government: National and regional governments play a central role in establishing regulatory frameworks, providing financial incentives, and implementing policies that support DER expansion. Policymakers must also ensure the alignment of energy strategies with broader decarbonisation objectives.
2. Academia: Research institutions contribute by developing cutting-edge technologies, conducting feasibility studies, and analysing policy impacts. Academic research is essential for optimising DER integration, cybersecurity solutions, and energy system resilience.
3. Industry: Private sector participation is crucial for deploying DER technologies,

[31] Content on the cooperation between government, academia, and industry were covered in keynote addresses and presentations by Dr Masaki Umejima, Dr Selvakumar Manickam, and Prof. Karen Morgan.

investing in infrastructure, and creating viable business models. Energy companies, technology firms, and service providers must work closely with regulators and researchers to address operational challenges and market barriers.

Strengthening partnerships amongst these sectors will facilitate knowledge-sharing, capacity-building, and the implementation of best practices across ASEAN. Additionally, cross-border collaboration and international standardisation efforts will be necessary to harmonise DER policies and technological advancements within the region.

2.4. Importance of Cybersecurity in the DER Landscape

As DER adoption expands, the energy sector faces an increased risk of cyber threats. The digitalisation of energy systems, integration of IoT devices, and real-time communication networks create vulnerabilities that malicious actors could exploit. Cybersecurity must, therefore, be a top priority in the transition to decentralised energy systems.

Key cybersecurity considerations include:

- Resilience against cyber threats: Energy networks must be designed with robust security measures to prevent cyberattacks that could disrupt power supply and compromise critical infrastructure.
- Standardised security frameworks: Implementing international cybersecurity standards, such as the Cyber-Physical Security Framework (CPSF), will help ASEAN nations establish a unified defence against cyber risks.
- Capacity building and training: Enhancing cybersecurity awareness amongst energy professionals, policymakers, and technology developers is essential for maintaining a secure energy ecosystem.
- Collaboration and information sharing: Governments, industries, and research institutions must work together to exchange intelligence on emerging cyber threats and best practices for mitigating security risks.

Without strong cybersecurity measures, DERs could become points of vulnerability rather than assets for energy resilience. Therefore, integrating cybersecurity considerations into DER policies, infrastructure development, and market operations is crucial for ensuring the long-term sustainability of decentralised energy systems.

2.5. Creating Cybersecurity Standards for DERs in the ASEAN Region

Establishing standards for cybersecurity for DERs is crucial for ensuring the safety, operability, and regulatory consistency. This requires a structured phased approach that incorporates best practices from referencing international standards and applying them in each country's context.

Steps toward creating cybersecurity standards for DERs in the ASEAN region:

1. Identify relevant documents for reference: ASEAN nations must first identify the major guidelines or standards pertaining to cybersecurity for DERs released by international standardisation organisations or other countries. Current standards which may serve as reference include the Cyber Physical Security Framework or Cybersecurity Guidelines for ERAB released by Japan.
2. Pick out best practices for application: Dedicated cybersecurity working groups composed of policymakers, industry experts, and academic researchers should be involved in identifying the best practices from these guidelines or standards and evaluate their applicability in their country's context.
3. Carry out localised tests in sandbox environments: Proof-of-concept tests should then be carried out, applying the key learning points and best practices from these reference guidelines or standards, in enclosed environments to test their feasibility in the local context. Results of these tests should be incorporated into the working groups' findings and submitted to relevant national agencies.
4. Create certification and compliance mechanisms: Each country's national agencies can then create a standardised certification programme, based on the key best practices and finding from the proof-of-concept tests, to ensure that DER technologies and operators comply with agreed-upon cybersecurity protocols.
5. Continuous monitoring and adaptation: On top of establishing a set of national standards or guidelines, there is also a need to establish a continuous monitoring mechanism, as cybersecurity threats evolve rapidly, thereby necessitating regular updates. This will help ASEAN nations to keep abreast of the latest events and stay ahead of emerging risks.

By following these steps, ASEAN countries can effectively develop a set of standards for cybersecurity for DERs that are based on international standards and customised for the local context. These efforts will contribute to the security of DERs and the decarbonisation goals for each country.

2.6. Community of Stakeholders for ERAB and its Cybersecurity

For DERs, ERAB and relevant cybersecurity initiatives to take root in the ASEAN region, it is essential to have a dedicated core of experts and stakeholders who will be involved in research, planning, policymaking, communicating, and managing all stages of the value chain. For this to happen, different government agencies from ASEAN Member States can create a shared platform to enable knowledge sharing, so that they are able to learn from one another's research, tests, and efforts related to the introduction, implementation, and management of DER, ERAB or relevant cybersecurity initiatives. Continuous collaboration within the community will allow for efforts to consistently build upon one another, and duplicate efforts will not be carried out, thereby maximising positive effects of cooperation.

Besides, this dedicated community will also be able to present a united front when

elevating any regional standards to the global arena. The community will be able to play the role of representatives when applying and communicating these standards to international standardisation organisations.

The five study groups have allowed for this budding community to be created, as experts from government, academia, industry, and community have gathered and agreed on the use of the CPSF, as well as the shared understanding of the Basic Concept of Cybersecurity for Distributed Energy Resources.

2.7. The Immediate Next Steps

Suggestions for the immediate next steps were included in the 5th study group as Prof. Masaki Umejima summarised as below:

- Formulate a policy framework that bridges national cybersecurity priorities with regional energy governance needs, offering regulatory guidance tailored to local contexts.
- Draft technical standards and operational procedures (SOPs) based on multilayered risk mapping of subsystem components within the Smart System 4 Layers.
- Design and deploy a role-based education and training platform to increase awareness, preparedness, and professional capacity in managing cyber-physical threats.
- Build a community of experts: researchers, lecturers, industry professionals, and policymakers, to help design and apply CPS security policies.
- Produce useful results such as a white paper, research papers, and a national roadmap for CPS (Cyber Physical System) security.
- Analyse the existing electricity market
    - Examine the current structure of the local electricity market, including energy generation, distribution, technologies, policy, and business mechanisms.
    - Identify challenges and constraints that hinder the integration of Distributed Energy Resources (DERs).
- Evaluate the feasibility of ERAB transition
    - Assess technical readiness, economic implications, regulatory gaps, and stakeholder dynamics involved in shifting from a centralised to a decentralised energy model.
    - Design a DER system architecture with CPSF compliance

    - Design a system architecture that supports DER integration aligned with Cyber-Physical System Functions (CPSF), emphasising cybersecurity, privacy, interoperability, and resilience.

- Design a Centralised Discovery Service (CDS): To explore the feasibility and design of a CDS, managed by a dedicated authority (e.g. the 'Echonet Lite Security Consortium'), to provide:
    - Controlled Access: Ensuring only authorised devices and entities can participate in the ERAB ecosystem.
    - Robust Authentication and Authorisation: Mechanisms for verifying identities and granting appropriate access privileges.
    - Secure Device Registration and Management: A centralised system for managing device credentials and maintaining an up-to-date registry of trusted devices.
- Define Trustworthiness and Accountability: To establish a clear framework for trust and accountability within the ERAB ecosystem by:
    - Defining Roles and Responsibilities: Clearly outlining the obligations of stakeholders (energy companies, aggregators, consumers, regulatory bodies).
    - Establishing Accountability Measures: Developing mechanisms for addressing security breaches and privacy violations, including incident response protocols and potential penalties.
- Develop a smart building–based testbed to simulate cyber-physical interactions within energy-related activities, including supply, demand, and distribution management, and to evaluate security vulnerabilities in a real-world, multilayered infrastructure.
- Adapt CPSF (Cyber Physical Security Framework) for each country.
    - Develop a model to identify risks in cyber-physical systems, based on the three layers (organisation, cyber-physical interaction, and cyberspace) and six key elements (organisation, people, devices, data, processes, and systems).

Chapter 4
Basic Concept for ASEAN to Strengthen Cybersecurity Measures for Distributed Energy Resources

1. Basic Concept of Cybersecurity for Distributed Energy Resources

Achieving robust cybersecurity for distributed energy resources (DERs) across ASEAN requires a shared concept that aligns all stakeholders on common principles, risk assessments, and security frameworks. Establishing this foundation is essential to ensuring interoperability, securing infrastructure, and facilitating cross-border energy transactions.

Building consensus on cybersecurity for DERs involves engaging key stakeholders, including government agencies, energy regulators, industry players, and academic researchers. The following steps may be considered for establishing a unified approach:

1. Defining common cybersecurity objectives: ASEAN countries must agree on core cybersecurity objectives, such as data integrity, system resilience, threat detection, and incident response for DERs.
2. Leveraging international standards: While ASEAN nations have different cybersecurity capabilities, aligning with international standards from organisations such as IEC ensures a minimum baseline for cybersecurity across the region.
3. Developing a risk-based framework: Stakeholders should collaborate to identify key vulnerabilities in DERs and create a risk-based security framework that prioritises high-impact threats.
4. Regional cybersecurity dialogues: ASEAN should establish forums for regular discussions, where stakeholders can exchange insights on emerging threats, regulatory developments, and best practices.
5. Pilot initiatives: Implementing joint cybersecurity pilot programmes in selected ASEAN countries will provide practical insights into implementation challenges and help refine regional security measures.

By building consensus through these initiatives, ASEAN nations can move toward a harmonised cybersecurity framework for DERs that balances national interests with regional cooperation.

2. Proposed Action Plan for the Realisation of Cybersecurity Systems for Distributed Energy Resources

While a shared cybersecurity concept is essential, each ASEAN country has distinct energy infrastructures, regulatory landscapes, and cybersecurity readiness levels. This was a key point raised in the Study Groups as well. As such, customising the action plan for each country ensures that policies and measures are adapted to local conditions.

The following action plan will serve as a potential guide for the realisation of the Basic Concept covered in the previous subchapter 4-1.

A key first step in customising cybersecurity action plans is conducting a thorough assessment of each country's:

- Distributed energy utilisation rates: Evaluating the level of DER integration, including the share of renewables, storage solutions, and smart grid technologies.
- Cybersecurity maturity: Assessing national cybersecurity policies, existing regulations, and institutional capabilities.
- Regulatory and market structures: Understanding how electricity markets operate and identifying gaps in cybersecurity enforcement.

Based on these assessments, each country's action plans can be customised with:

1. Policy adaptations: Countries with strong cybersecurity regulations can focus on DER-specific adaptations, while others may need foundational cybersecurity laws.
2. Capacity building programmes: Nations with lower cybersecurity readiness should receive support through targeted training, knowledge-sharing workshops, and cybersecurity drills.
3. Technical assistance: ASEAN-wide task forces can provide technical expertise to member states in developing secure DER architectures and conducting vulnerability assessments.
4. Public–private collaboration efforts: Encouraging partnerships between governments and industry players ensures that cybersecurity measures align with operational realities.

Next, to fully realise a regional cybersecurity framework for DERs, ASEAN nations must engage in coordinated efforts that promote information sharing, best practice dissemination, and legal harmonisation.

- Information sharing mechanisms: Effective cybersecurity requires a robust mechanism for sharing intelligence on cyber threats and vulnerabilities. Some measures to coordinate efforts include establishing a regional cybersecurity information exchange platform to facilitate real-time threat intelligence sharing,

implementing incident reporting standards to document and address security breaches, and leverage existing networks such as the ASEAN Regional CERT to improve cyber incident coordination.

- Best practice dissemination: Sharing cybersecurity best practices across ASEAN will help countries with lower cybersecurity readiness levels improve their defences. Some strategies to do so include the creation of ASEAN cybersecurity workshops, compilation of case studies, as well as carrying out cross-border technical training.
- Work towards a legally binding agreement: Ultimately, the ASEAN countries could work towards establishing a legally binding cybersecurity agreement that standardises cybersecurity requirements for DERs across the region. This would involve the drafting of an ASEAN Cybersecurity Framework for DERs to outline minimum security requirements for DER operators and aggregators and the implementation of mutual recognition agreements (MRAs) for the recognition of cybersecurity certifications and standards across the ASEAN region.

Chapter 5
Recommendations for the Expansion of DERs, Adoption of ERAB, and Implementation of Relevant Cybersecurity Standards

1. Recommendations for the Expansion of DERs and Adoption of ERAB

DERs offer ASEAN countries the possibility to improve grid flexibility by removing the dependence on large traditional power plans and long transmission lines. At the same time, they also accelerate the transition to a low-carbon economy, as renewable energy technologies leveraging solar and wind energies do not produce any carbon emissions at the point of generation.

In order to expand the implementation of DERs, stakeholders need to be aware of these benefits. However, awareness alone will not drive its adoption, as clear economic and reliability benefits from participating in decentralised energy systems for both energy suppliers and consumers need to be shown.

This is where this project and the five study groups come in, as stakeholders along the entire energy generation and distribution value chain across different ASEAN countries have agreed on the importance of DERs. The next step is to work with policymakers to update relevant regulations or pass new ones to fully value the services that DERs can provide.

Moving beyond DERs, it has also been analysed that aggregators have an important role to play as well. Their ability to manage and optimise multiple DERs under a single allow them to improve grid efficiency and facilitate more participation in energy markets, demand response programmes, and grid balancing services. This means that incumbent grid operators and stakeholders along the value chain as well as new market entrants can also participate in the market, thereby providing new economic opportunities.

2. Recommendations for the Implementation of Cybersecurity Standards and Referencing Guidelines for DER and ERAB

As covered in the previous chapters, it is essential for stakeholders to recognise and share a common understanding regarding cybersecurity objectives for distributed energy resources and ERAB. The five study groups have kickstarted this process, culminating in the creation of the Basic Concept of Cybersecurity for Distributed Energy Resources, which participants of the study groups and the organisations that they represent have agreed upon.

This forms the basis for the creation of a platform for ASEAN stakeholders in government, industry, academia, and community to come together to work on the development of relevant frameworks, taking reference from Japan's Cyber Physical Security Framework (CPSF) and ERAB Guidelines, and customising them for every country's context.

In the meantime, stakeholders involved in research can embark upon the tasks highlighted in the 5th study group (refer to Chapter 3-2-6). These include the formulation of policy frameworks, drafting of technical standards, designing education and awareness programmes, as well as building a community of experts.

With this project and the culmination of the five study groups, the ASEAN region moves towards the creation of a set of robust cybersecurity standards for distributed energy resources and ERAB which can be flexibly adapted to each country's context, taking into account every country's economic and social situation. ASEAN is poised to elevate this set of standards to the international arena, where other countries around the world can learn from the best practices and insights from ASEAN stakeholders. This can be carried out through applying the standards to international standardisation organisations such as the IEC and ISO, where the standards will have a much larger exposure to the rest of the world.

3. Final Recommendations

Having thoroughly evaluated the issues and bottlenecks relating to DES and ERAB, a multifaceted approach targeting all relevant stakeholders is necessary for the development of cybersecurity measures and promotion of DES and ERAB in the ASEAN region. This study provides the following recommendations for the expansion of DERs, as well as the development of cybersecurity measures and the promotion of DERs and ERAB, in conjunction with ACE's recommendations in the 8th ASEAN Energy Outlook[32]:

Table 5.1 Proposed Recommendations for the Expansion of DERs

Recommendation	Details
Policy Framework	• Establish a clear framework for trust and accountability within the ERAB ecosystem by defining roles and responsibilities as well as establishing accountability measures • Analyse continuously the existing electricity market in each country to understand current local structures, including energy generation, distribution, technologies, policy and business mechanisms • Implement effective policies to liberalise the energy market and allow for new business models such as the energy resource aggregation businesses (ERAB) • Support coordination with local power companies and related organisations

[32] ACE, 8th Energy Outlook.

Government Support	• Orchestrate policies and market rules at all levels of the power system • Provide help to ensure compliance towards local standards and business environments
Grid Integration	• Strength power system infrastructure to allow for smooth DER integration • Address cost-reliability trade-offs for grid-connected renewable energy technologies • Implement security-by-design principles during grid integration
Local and Regional Supply Chain Development	• Expand and establish regional supply chains • Regional and international collaboration on research and development, technology, and knowledge transfer

Source: Created by authors, extracted from the conclusion of the fifth study group

Table 5.2 Proposed Recommendations for the Development of Cybersecurity Measures and the Promotion of DERs and ERAB

Recommendation	Details
Adoption and Adaptation of CPSF	• Develop a model to identify risks in cyber-physical systems, based on the three layers of organisation, cyber-physical interaction, and cyberspace, and the six key elements of organisation, people, devices, data, processes, and systems • Analyse each country's context and the feasibility of adapting the CPSF to each ASEAN country
Technical Standard	• Draft technical standards and standard operational procedures (SOPs) based on multilayered risk mapping of subsystem components • Refer to documents such as the CPSF and ERAB guidelines for the drafting of such technical standards
Policy and Financial Incentives	• Formulate a policy framework that connects cybersecurity priorities with regional energy governance needs • Provide support for compliance with cybersecurity guidelines pertaining to the energy sector
Government Support	• Support for development and adaptation with international standards and specifications or guidelines such as the 'ERAB Security Guidelines' to improve cybersecurity for the energy sector
Community	• Build a community of experts, including researchers, lecturers, industry professionals, and policymakers, to help design and apply cyber physical system security policies

	• Produce white papers, research papers, and aid in the creation of national roadmaps for cyber physical system security
Local and Regional Supply Chain Development	• Creation of shared resources to enable timely information sharing on cyber incidents in the energy sector in the ASEAN region

Source: Created by authors, adapted from 8th ASEAN Energy Outlook

References

360info (2024), Southeast Asia's three-nation partnership to fight cyber threats. https://360info.org/southeast-asias-three-nation-partnership-to-fight-cyber-threats/ (accessed 5 September 2024).

AA (2023), National Security Strategy. https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf (accessed 22 August 2024).

ABNR Law (2024), Indonesia Issues New Rules on Operation of Rooftop Solar, Abolishes Net Metering. https://www.abnrlaw.com/news/indonesia-issues-new-rules-on-operation-of-rooftop-solar-abolishes-net-metering (accessed 22 August 2024).

ACSC (2022), Who we are. Canberra. https://www.cyber.gov.au/about-us/about-asd-acsc/who-we-are (accessed 23 August 2024).

Advisera (2024), What is NIS 2 Directive? A detailed and straightforward guide. https://advisera.com/articles/what-is-nis2/ (accessed 18 September 2024).

AEMO (2024), AESCSF framework and resources. https://aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources (accessed 23 August 2024).

Air Carbon Exchange (n.d.), ACX Singapore. https://acx.net/acx-singapore/ (accessed 1 August 2024).

ANRE (2023), Policies. https://www.enecho.meti.go.jp/en/category/ (accessed 24 August 2024).

ARENA (2024), Distributed Energy Integration Program (DEIP). https://arena.gov.au/knowledge-innovation/distributed-energy-integration-program/ (accessed 23 August 2024).

ASD (2023), ASD Cyber Threat Report 2022-2023. Canberra. https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023 (accessed 23 August 2024).

ASEAN (2021), ASEAN Cybersecurity Cooperation Strategy (2021-2025). https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf (accessed 27 August 2024).

ASEAN Briefing (2022), Indonesia's Positive Investment List: Sectors Open and Restricted to Foreign Businesses. https://www.aseanbriefing.com/news/indonesias-positive-investment-list-and-the-sectors-open-restricted-to-foreign-businesses/ (accessed 21 August 2024).

ASEAN Briefing (2023), Philippines Opens Renewable Energy to Full Foreign Ownership. https://www.aseanbriefing.com/news/philippines-opens-renewable-energy-to-full-foreign-ownership/ (accessed 2 August 2024).

ASEAN Centre for Energy (ACE) (2024), ACE in ASEAN Energy Sector. https://aseanenergy.org/about/introduction/ (accessed 27 August 2024).

ASEAN Centre for Energy (ACE) (2024), 8th ASEAN Energy Outlook. Jakarta. https://aseanenergy.org/wp-content/uploads/2024/09/8th-ASEAN-Energy-Outlook.pdf (accessed 17 March 2025).

ASEAN Energy Database System (2020), Philippines steps up security to shield power grid from foreign control. https://aseanenergy.org/news-clipping/philippines-steps-up-security-to-shield-power-grid-from-foreign-control/ (accessed 30 July 2024).

ASEAN Energy Database Systems (n.d.), Vietnam abandons net-metering method for rooftop solar projects. https://aseanenergy.org/news-clipping/vietnam-abandons-net-metering-method-for-rooftop-solar-projects/ (accessed 5 September 2024).

ASEAN-German Energy Programme (2016), RE Market in Brunei Darussalam. https://agep.aseanenergy.org/country-profiles/brunei-darussalam/brunei-re-sector/#1526611060469-668e6341-e2e4 (accessed 13 August 2024).

Asia Business Law Journal (2021), Renewable energy regulations in Malaysia. https://law.asia/renewable-energy-regulations-malaysia/ (accessed 5 August 2024).

Asia Law Portal (2019), Cybersecurity Law: Thailand. https://asialawportal.com/cybersecurity-law-in-thailand/ (accessed 5 September 2024).

Asia Pacific Foundation of Canada (2024), Indonesian Government Under Fire Following String of Cyber Breaches. https://www.asiapacific.ca/publication/indonesian-government-under-fire-after-cyber-breaches (accessed 18 August 2024).

Asian Development Bank (2021), How Different Electricity Pricing Systems Affect the Energy Trilemma: Assessing Indonesia's Electricity Market Transition. https://www.adb.org/publications/how-different-electricity-pricing-systems-affect-energy-trilemma-indonesia (accessed 19 August 2024).

Asian Development Bank (ADB) (2024), Southeast Asia Energy Transition Partnership (formerly Southeast Asia Green Recovery Program). https://www.adb.org/projects/58029-001/main (accessed 5 September 2024).

Austin Chamber (2023), We must protect our energy industry from cyberattacks – together. https://www.austinchamber.com/blog/we-must-protect-our-energy-industry-from-cyberattacks-together (accessed 21 August 2024).

Australia Strategic Policy Institute (2022), Australia and Indonesia should work to deepen cyber ties. Australia. https://www.aspistrategist.org.au/australia-and-indonesia-should-work-to-deepen-cyber-ties/ (accessed 20 August 2024).

Badan Siber dan Sandi Negara-BSSN (2023), Lanskap Keamanan Siber 2023. Jakarta. https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf (accessed 18 September 2024).

Baker McKenzie (2024), Vietnam: Draft new circular on the Vietnam wholesale electricity market's regulations and its implications for power projects. https://insightplus.bakermckenzie.com/bm/attachment_dw.action?attkey=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQJsWJiCH2WAWE%2FeOkjb67%2BkrsXbalVGif&nav=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQbuwypnpZjc4%3D&attdocparam=pB7HEsg%2FZ312Bk8OIuOIH1c%2BY4beLEAe7RAboBpJzFs%3D&fromContentView=1 (accessed 9 September 2024).

Bangkok Post (2024), ASEAN-Japan Cybersecurity Meeting Boosts Regional Collaboration. https://www.bangkokpost.com/thailand/pr/2737396/asean-japan-cybersecurity-meeting-boosts-regional-collaboration (accessed 5 September 2024).

Bangkok Post (2024), Thailand tops region for ransomware attacks. https://www.bangkokpost.com/business/general/2792735/thailand-tops-region-for-ransomware-attacks (accessed 5 September 2024).

Bastille Post (2024), Defending Malaysia's cybersecurity: Group-IB and CyberSecurity Malaysia forge strategic alliance to safeguard national cyber resilience. https://www.bastillepost.com/global/article/4057698-defending-malaysias-cybersecurity-group-ib-and-cybersecurity-malaysia-forge-strategic-alliance-to-safeguard-national-cyber-resilience (accessed 5 September 2024).

Berakas Power Company (2024), Core Business. Brunei Darussalam. https://www.bpc-brunei.com/aboutus/#core-business (accessed 24 July 2024).

Bird & Bird (2024), Solar Energy & Corporate PPAs in Singapore. https://www.twobirds.com/en/insights/2024/singapore/solar-energy-corporate-ppas-in-singapore (accessed 31 July 2024).

Brunei Department of Energy (2022), Guidebook: Solar PV Rooftop and Net-Metering Programme. Brunei Darussalam. https://www.energy.gov.bn/Shared%20Documents/Resources/SOLAR%20PV%20GUIDEBOOK%20ENG.pdf (accessed 19 September 2024).

BSI (2021), Second act on increasing the security of IT systems (German IT Security Act 2.0). https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordungen/IT-SiG/2-0/it_sig_2-0.html (accessed 22 August 2024).

BSI (2023), The State of IT Security in Germany in 2023. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Security situation/IT-Security-Situation-in-Germany-2023.pdf?__blob=publicationFile&v=8 (accessed 22 August 2024).

BSI (2024), KRITIS and regulated companies. https://www.bsi.bund.de/EN/Themen/KRITIS-und-regulierte-

Unternehmen/kritis-und-regulierte-unternehmen_node.html (accessed 22 August 2024).

Bursa Carbon Exchange (2023), BURSA CARBON EXCHANGE SUCCESSFULLY COMPLETES MALAYSIA'S INAUGURAL CARBON AUCTION. Malaysia. https://bcx.bursamalaysia.com/index.php?rp=bcx_pressrelease_17march2023 (accessed 7 August 2024).

Bursa Karbon Indonesia (IDX Carbon) (n.d.), About Us. Indonesia. https://idxcarbon.co.id/id (accessed 26 August 2024).

Capital IQ (n.d.), Country Power Generation by Fuel Type. Paid Database (accessed 29 July 2024).

CISC (2023), Critical Infrastructure Resilience Strategy. https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf (accessed 23 August 2024).

CISC (2024), About us. https://www.cisc.gov.au/about-us (accessed 23 August 2024).

CISC (2024), Security of Critical Infrastructure Act 2018 (SOCI). https://www.cisc.gov.au/legislation-regulation-and-compliance/soci-act-2018 (accessed 23 August 2024).

Climate Impact X (n.d.), CIX Exchange. https://www.climateimpactx.com/exchange (accessed 1 August 2024).

CNN Indonesia (2023), Kominfo Klarifikasi Soal Dugaan Bocoran Data BSI yang Beredar. Jakarta. https://www.cnnindonesia.com/teknologi/20230522122857-192-952382/kominfo-klarifikasi-soal-dugaan-bocoran-data-bsi-yang-beredar (accessed 25 August 2024).

Coherent Market Insights (2024), Singapore's Carbon Credit Market Surging At 21% CAGR. https://carboncredits.com/singapores-carbon-credit-market-surging-at-21-cagr/ (accessed 31 July 2024).

CSA (2022), Cybersecurity Code of Practice for Critical Information Infrastructure - Second Edition. https://www.csa.gov.sg/docs/default-source/legislation/ccop_second-edition.pdf?sfvrsn=b2ab666a_2 (accessed 3 October 2024).

CSA (2023), Singapore Cyber Landscape 2022. https://www.csa.gov.sg/Tips-Resource/publications/2023/singapore-cyber-landscape-2022 (accessed 3 October 2024).

CSA (2024), 2024 OTCEP Members. https://www.otcep.gov.sg/2024-otcep-members/ (accessed 3 October 2024).

CSA (2024), Cybersecurity Act. https://www.csa.gov.sg/legislation/Cybersecurity-Act (accessed 3 October 2024).

CSA (2024), Cybersecurity Labelling Scheme (CLS). https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme (accessed 3 October 2024).

CSA (2024), Operational Technology Cybersecurity Expert Panel. https://www.csa.gov.sg/Explore/who-we-are/committees-and-

panels/operational-technology-cybersecurity-expert-panel (accessed 3 October 2024).

CSA (2024), Singapore Cyber Landscape 2023. https://www.csa.gov.sg/Tips-Resource/publications/2024/singapore-cyber-landscape-2023 (accessed 3 October 2024).

CSA (2024), Singapore's Operational Technology Cybersecurity Masterplan 2024. https://www.csa.gov.sg/Tips-Resource/publications/2024/operational-technology-cybersecurity-masterplan-2024 (accessed 3 October 2024).

CSA (2024), What We Do. https://www.csa.gov.sg/Explore/what-we-do (accessed 3 October 2024).

Cyber Security Agency of Singapore (CSA) (2024), Singapore Moves Ahead to Establish the ASEAN Regional CERT to Strengthen Regional Cybersecurity. https://www.csa.gov.sg/News-Events/Press-Releases/2024/singapore-moves-ahead-to-establish-the-asean-regional-cert-to-strengthen-regional-cybersecurity (accessed 27 August 2024).

Cybersecurity ASEAN (2023), Malaysia Holds Top Three Spot for Phishing Attacks in Southeast Asia. https://cybersecurityasean.com/news-press-releases/malaysia-holds-top-three-spot-phishing-attacks-southeast-asia (accessed 28 August 2024).

CyberSecurity Malaysia (2020), CyberSecurity Malaysia Annual Report 2020. https://www.cybersecurity.my/data/content_files/46/2464.pdf (accessed 4 September 2024).

Danish Energy Agency (2022), Demand Response in Vietnam. https://ens.dk/sites/ens.dk/files/Globalcooperation/demand_response_in_vietnam_-_deliverable_2.1.pdf (accessed 10 September 2024).

Data Center Dynamics (2021), Facebook to buy renewable energy from offshore floating solar farm in Singapore. https://www.datacenterdynamics.com/en/news/facebook-to-buy-renewable-energy-from-offshore-floating-solar-farm-in-singapore/ (accessed 31 July 2024).

Dave Seibert-DFDL (2024), Cambodia: New Article 6 Regulations - Opportunities in the Carbon Credit Market. Cambodia. https://www.dfdl.com/insights/legal-and-tax-updates/cambodia-new-article-6-regulations-opportunities-in-the-carbon-credit-market/ (accessed 28 July 2024).

DefenseOne (2023), US, Indonesia expand defense cooperation, starting with cyber and space. USA. https://www.defenseone.com/defense-systems/2023/11/us-indonesia-expand-defense-cooperation-starting-cyber-and-space/392104/ (accessed 20 August 2024).

Department of Energy Philippines (2015), Retail Competition and Open Access (RCOA). Philippines. https://doe.gov.ph/philippine-grid-net-generation?q=rcoa (accessed 2 August 2024).

Department of Energy Philippines (2019), Annex 1: Smart Distribution Utility Roadmap (SDUR). Philippines.

https://doe.gov.ph/sites/default/files/pdf/announcements/draft_dc_12_july_2019_annex_a_sdu_roadmap_for%20_dus.pptx (accessed 2 August 2024).

Department of Energy Philippines (2020), 2019 Power Situation Report. Philippines. https://doe.gov.ph/sites/default/files/pdf/electric_power/2019-power-situation-report.pdf (accessed 1 August 2024).

Department of Energy Philippines (2020), Department Circular No. DC2020-02-0003. Philippines. http://doe.gov.ph/sites/default/files/pdf/issuances/dc2020-02-0003.pdf (accessed 2 August 2024).

Department of Energy Philippines (2021), Guidebook on Net Metering in the Philippines. Philippines. https://doe.gov.ph/sites/default/files/pdf/announcements/draft-guidebook-on-net-metering-2021.pdf (accessed 2 August 2024).

Department of Energy Philippines (2022), Green Energy Option Program (GEOP). Philippines. https://doe.gov.ph/sites/default/files/pdf/consumer_connect/Primer%20on%20Green%20Energy%20Option%20Program.pdf (accessed 2 August 2024).

Department of Energy, Philippines (2018), Philippine Energy Plan 2018-2040. https://policy.asiapacificenergy.org/sites/default/files/Philippine%20Energy%20Plan%202018-2040.pdf (accessed 31 July 2024).

Department of Energy, Philippines (2020), Department Circular No. DC2020-02-0003: Prescribing the policy for the Transparent and Efficient Procurement of Ancillary Services by the System Operator. https://policy.thinkbluedata.com/sites/default/files/Department%20Circular%20No.%20DC2020-02-0003.pdf (accessed 31 July 2024).

Department of Information and Communications Technology, Philippines (2024), National Cybersecurity Plan 2023-2028. https://dict.gov.ph/wp-content/uploads/2024/02/NCSP-2023-2028-FINAL.pdf (accessed 31 July 2024).

Department of Justice (n.d.), Office of Cybercrime. https://www.doj.gov.ph/office-of-cybercrime.html (accessed 31 July 2024).

Directorate of Investment and Company Administration (2017), The Notification No.15/20187 on the List of Restricted Investment Activities. Myanmar. https://www.dica.gov.mm/en/news/announcement-notification-list-restricted-investment-activities (accessed 30 July 2024).

Duong Ngoc Thai (2020), Vietnam has no choice but to counter China's cyber thuggery. https://e.vnexpress.net/news/perspectives/vietnam-has-no-choice-but-to-counter-china-s-cyber-thuggery-4107109.html (accessed 5 September 2024).

Electricity Generating Authority of Thailand (n.d.), EGAT Profile. Thailand. https://www.egat.co.th/home/en/about-egat/ (accessed 8 August 2024).

Electricity Subsector Coordinating Council (2024), ESCC Overview. https://www.electricitysubsector.org/ (accessed 20 August 2024).

EMA (2024), Our Role as a Power System Operator. https://www.ema.gov.sg/about-ema/who-we-are/our-role-as-a-power-system-operator (accessed 3 October 2024).

Energy Market Authority (2022), Enhancing the Demand Response (DR) and Interruptible Load (IL) Programmes with a Demand Side Management Sandbox. Singapore. https://www.ema.gov.sg/content/dam/corporate/our-energy-story/energy-demand/factsheet-demand-response-interruptible-load_20221103.pdf (accessed 30 July 2024).

Energy Market Authority (2024), Energy Market Landscape. Singapore. https://www.ema.gov.sg/our-energy-story/energy-market-landscape/electricity (accessed 30 July 2024).

Energy Market Authority (2024), Solar - Solar Installation Guide. Singapore. https://www.ema.gov.sg/consumer-information/solar/solar-installation-guide (accessed 31 July 2024).

Energy Market Company (2024), NEMS Market Report 2023. Singapore. https://www.home.emcsg.com/publications/-/media/Comms/NEMS-Market-Reports/NEMS-Market-Report-2023_Final_3.pdf (accessed 30 July 2024).

ERIA (2017), Electric Power Policy and Market Structure in ASEAN Member States pp.3 - 46. Jakarta. http ://www.eria.org/RPR_FY2015_No.18 _Chapter_2 .pdf (accessed 23 July 2024).

ERIA (2021), Clean Electricity Supply: Temburong Ecotown Development Phase 4 pp.32-81. Jakarta. 0 (accessed 19 September 2024).

EUR-Lex (2022), Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454 (accessed 18 September 2024).

EVN - NLDC (2019), VIETNAM WHOLESALE ELECTRICITY MARKET (VWEM) OVERVIEW. Viet Nam. https://vepg.vn/wp-content/uploads/2019/09/3.-DPPA_VNWholesaleElecMarket_EVNNLDC_20190612_En.pdf (accessed 10 September 2024).

EVN - NLDC (2021), VIETNAM WHOLESALE ELECTRICITY MARKET 2021. Viet Nam. https://vepg.vn/wp-content/uploads/2021/05/NLDC_VWEM-2021-22042021.pdf (accessed 9 September 2024).

EVN - NLDC (2023), UPDATES ON VIETNAM POWER SYSTEM AND ELECTRICITY MARKET OPERATION. Vietnam. https://vepg.vn/wp-content/uploads/2023/06/EN_NLDC_Updates-on-Vietnam-Power-System-and-Electricity-Market.pdf (accessed 2 September 2024).

EVN (2023), WHOLESALE ELECTRICITY TARIFF. Viet Nam. https://en.evn.com.vn/d6/news/WHOLESALE-ELECTRICITY-TARIFF-9-28-260.aspx (accessed 11 September 2024).

EVN (2024), Annual Report 2022 - 2023. Viet Nam. https://en.evn.com.vn/userfile/User/huongBTT/files/2024/5/EVNAnnualReport2022%202023.pdf (accessed 9 September 2024).

Federal Energy Regulatory Commission (2024), What is FERC?. https://www.ferc.gov/what-ferc-does (accessed 20 August 2024).

Fitch Solutions (2024), Indonesia Power & Renewables Report. https://store.fitchsolutions.com/power-renewables/indonesia-power-renewables-report (accessed 22 August 2024).

Fitch Solutions (2024), Malaysia Power & Renewables Report. https://store.fitchsolutions.com/power-renewables/malaysia-power-renewables-report (accessed 6 August 2024).

Fitch Solutions (2024), Philippines Power & Renewables Report. https://store.fitchsolutions.com/power-renewables/philippines-power-renewables-report (accessed 1 August 2024).

Fitch Solutions (2024), Singapore Power & Renewables Report. https://store.fitchsolutions.com/power-renewables/singapore-power-renewables-report (accessed 30 July 2024).

Fitch Solutions (2024), Thailand Power & Renewables Report. https://store.fitchsolutions.com/power-renewables/thailand-power-renewables-report (accessed 12 August 2024).

Fitch Solutions (2024), Vietnam Power & Renewables Report. https://store.fitchsolutions.com/power-renewables/vietnam-power-renewables-report (accessed 3 September 2024).

Fulcrum (2024), Strengthening ASEAN-Japan cybersecurity cooperation. https://fulcrum.sg/strengthening-asean-japan-cybersecurity-cooperation/ (accessed 9 September 2024).

GGGI (2024), Government of Lao PDR holds multi-stakeholder consultation on the draft Decree on Carbon Credits. Lao PDR. https://gggi.org/government-of-lao-pdr-holds-multi-stakeholder-consultation-on-the-draft-decree-on-carbon-credits/ (accessed 21 August 2024).

GlobalSign (2023), The Cybersecurity Improvement Act 2020 & NIST Cybersecurity For IoT. https://www.globalsign.com/en/blog/cybersecurity-improvement-act-nist-iot (accessed 18 September 2024).

GMA Integrated News (2024), DOE-GEMP latest gov't. website attacked by hackers. https://www.gmanetwork.com/news/topstories/nation/915003/doe-gemp-latest-gov-t-website-attacked-by-hackers/story/#goog_rewarded (accessed 30 July 2024).

Government of the Philippines (2019), Designating the Philippine Statistics Authority (PSA) as the sole agency to compile and release official national accounts of the Philippines (EO No. 95, s. 2019). https://lawphil.net/executive/execord/eo2019/pdf/eo_95_2019.pdf (accessed 31 July 2024).

GovTech (2023), Factsheet – Government Cyber Security Operations Centre (GCSOC). https://www.smartnation.gov.sg/media-hub/press-releases/gcsoc-factsheet/ (accessed 3 October 2024).

GovTech (2024), Safeguarding the Government's Information and Communications Technology & Smart Systems. https://www.tech.gov.sg/our-capabilities/cybersecurity/ (accessed 3 October 2024).

Green Finance & Development Center (2023), Vietnam's Eight National Power Development Plan (PDP8). https://greenfdc.org/vietnams-eight-national-power-development-plan-pdp8/ (accessed 15 September 2024).

IEA (2022), Energy System of Cambodia. https://www.iea.org/countries/cambodia (accessed 28 August 2024).

IEA (2022), Enhancing Indonesia's Power System. https://www.iea.org/reports/enhancing-indonesias-power-system (accessed 19 August 2024).

IEA (2024), Annual variable renewable energy share and corresponding system integration phase in selected countries/regions, 2022. https://www.iea.org/data-and-statistics/charts/annual-variable-renewable-energy-share-and-corresponding-system-integration-phase-in-selected-countries-regions-2022 (accessed 26 July 2024).

IEC (2020), IEC 61968-5. Geneva. https://webstore.iec.ch/en/publication/60069 (accessed 26 August 2024).

IEC (2024), IEC 61850 Series. Geneva. https://webstore.iec.ch/en/publication/6028 (accessed 26 August 2024).

IEC (2024), IEC 62351 Series. Geneva. https://webstore.iec.ch/en/publication/6912 (accessed 26 August 2024).

IEC (2024), Smart Energy Roadmap (based on IEC TR 63097). https://syc-se.iec.ch/iec-63097-smart-energy-roadmap/ (accessed 26 August 2024).

Independent Electricity Market Operator (n.d.), About the Philippine Electricity Market. Philippines. https://www.iemop.ph/the-market/ (accessed 1 August 2024).

Industrial Cyber (2024), US DHS partners with Indonesia to strengthen maritime cybersecurity in Indo-Pacific region. https://industrialcyber.co/transport/us-dhs-partners-with-indonesia-to-strengthen-maritime-cybersecurity-in-indo-pacific-region/ (accessed 18 August 2024).

International Finance Corporation (2021), Investment Reform Map for Lao PDR: A foundation for a New Investment Policy and Promotion Strategy. https://documents1.worldbank.org/curated/en/732601621326114842/pdf/Investment-Reform-Map-for-Lao-PDR-A-Foundation-for-a-New-Investment-Policy-and-Promotion-Strategy-Lao-PDR-Investment-Climate-Reform-Project.pdf (accessed 20 August 2024).

International Institute for Strategic Studies (IISS) (n.d), Cyber capabilities and national power: Vietnam. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---vietnam.pdf (accessed 5 September 2024).

International Journal of Electronics and Electrical Engineering (2020), De-Regulation of Electricity Industry: A Malaysian Perspective. https://www.ijeee.net/uploadfile/2020/0619/20200619112247349.pdf (accessed 5 August 2024).

International Monetary Fund, Asia and Pacific Dept (2023), Selected issues: Brunei Darussalam.

https://www.elibrary.imf.org/configurable/content/journals$002f002$002f2023$002f347$002farticle-A001-en.xml?t:ac=journals%24002f002%24002f2023%24002f347%24002farticle-A001-en.xml (accessed 20 September 2024).

International Trade Administration USA (2024), Vietnam - Power Generation, Transmission, and Distribution. https://www.trade.gov/country-commercial-guides/vietnam-power-generation-transmission-and-distribution (accessed 2 September 2024).

IPA (n.d.), Enabling digital transformations in industries and society. https://www.ipa.go.jp/en/digital/index.html (accessed 24 August 2024).

ISA/IEC (n.d.), ISA/IEC 62443 Series of Standards. North Carolina. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards (accessed 26 August 2024).

Japan International Cooperation Agency (JICA) (2024), JICA backs PH government's efforts in safeguarding cyberspace. https://www.jica.go.jp/english/overseas/philippine/information/press/2024/1545307_53492.html (accessed 2 August 2024).

Kaohoon (2022), BCP shows 95% of its carbon credit trading in the Thai market in the first half of the year. https://www.kaohoon.com/news/548871 (accessed 13 August 2024).

Kementerian ESDM (2021), Gandeng BSSN, Kementerian ESDM Bentuk Tim Tanggap Insiden Siber. Jakarta. https://www.esdm.go.id/id/media-center/arsip-berita/gandeng-bssn-kementerian-esdm-bentuk-tim-tanggap-insiden-siber (accessed 8 September 2024).

Legifrance (2018), LOI n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité (1). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000036644772 (accessed 22 August 2024).

Legifrance (2023), LOI n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense (1). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047914986 (accessed 22 August 2024).

Lexology (2022), Malaysia's Corporate Green Power Programme: Virtual Power Purchase To The Fore. https://www.lexology.com/library/detail.aspx?g=c65dbbc5-51ea-4af5-be55-91bd722c5bdc (accessed 6 August 2024).

Lexology (2024), Launch of the Direct Power Purchase Mechanism in Vietnam. https://www.lexology.com/library/detail.aspx?g=f8ce4664-eed9-49b1-80f2-09879c57bbe7 (accessed 6 September 2024).

Liputan 6 (2022), 11 Fakta Hacker Bjorka yang Retas Data Pemerintah Indonesia. Jakarta. https://www.liputan6.com/citizen6/read/5067854/11-fakta-hacker-bjorka-yang-retas-data-pemerintah-indonesia?page=2 (accessed 28 August 2024).

Malaysia Computer Emergency Response Team (MyCERT) (2023), Incident Statistics 2023. https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-

4d11-8169-66677d694932&id=2862eb40-2bc0-4b4e-90ed-07d4eef73b7b (accessed 3 August 2024).

Manila Bulletin (2022), Six months of phishing attacks in 2022 exceed SEA's total number last year. https://mb.com.ph/2022/10/12/six-months-of-phishing-attacks-in-2022-exceed-seas-total-number-last-year/ (accessed 28 August 2024).

METI (2019), Cybersecurity Guidelines for Energy Resource Aggregation Business Ver 2.0. Japan. https://www.enecho.meti.go.jp/en/category/vpp_dr/data/cybersecurity_guidelines_for_erab.pdf (accessed 24 August 2024).

METI (2019), The Cyber/Physical Security Framework. Japan. https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0_eng.pdf (accessed 24 August 2024).

Metropolitan Electricity Authority (2023), MEA extends application deadline for Demand Response Pilot Project for 2022-2023 to reduce power consumption in Category 3, 4 and 5 according to EPPO policy from now until 31 Oct 2022. Thailand. https://www.mea.or.th/en/public-relations/corporate-news-activities/announcement/hnzp7wxgL (accessed 16 August 2024).

Microsoft (2018), Microsoft and Sunseap sign agreement on largest-ever solar project in Singapore. https://news.microsoft.com/2018/02/28/microsoft-and-sunseap-sign-agreement-on-largest-ever-solar-project-in-singapore/ (accessed 31 July 2024).

MINDEF (2022), National Agencies Tackle Cyber Threats at Inaugural Cyber Defence Exercise; DIS and CSA Sign Joint Operations Agreement for Cyber Cooperation. https://www.mindef.gov.sg/news-and-events/latest-releases/16nov22_nr (accessed 3 October 2024).

Ministry of Energy (2015), THAILAND: Master Plan for Smart Grid Network System Development in Thailand 2015-2036. https://policy.asiapacificenergy.org/node/4348 (accessed 5 September 2024).

Ministry of Energy, Brunei Darussalam and ERIA (2023), Brunei Darussalam Country Report: Energy Outlook and Energy-Saving Potential in East Asia 2023. Jakarta. (accessed 20 September 2024).

Ministry of Information and Communications (2023), Sách trắng TÁ 2023. https://mic.mediacdn.vn/639352410187198464/2024/8/22/sach-trang-ta-2023-7-6-24-17243135905472033515302.pdf (accessed 5 September 2024).

Ministry of Information and Communications (MIC), Vietnam (n.d), Authority of Information Security. https://english.mic.gov.vn/authority-of-information-security-197114301.htm (accessed 5 September 2024).

Naebboon Hoonchareon, Chulalongkorn University, TH. (2015), Thailand Smart Grid Policy Plan and Roadmaps. https://policy.asiapacificenergy.org/sites/default/files/Master%20Plan%20for%20Smart%20Grid%20Network%20System%20Development%20in%20Thailand%202015-2036%20%28Presentation%29%20%28EN%29.pdf (accessed 5 September 2024).

Nation Thailand (2023), Household 'net energy metering' plan put on hold. Thailand. https://www.nationthailand.com/thailand/general/40029286 (accessed 13 August 2024).

National Association of Regulatory Utility Commissioners (2024), Cybersecurity Baselines for Electric Distribution Systems and DER. Washington, DC. https://www.naruc.org/core-sectors/critical-infrastructure-and-cybersecurity/cybersecurity-for-utility-regulators/cybersecurity-baselines/ (accessed 21 August 2024).

National CSIRT of Indonesia (2023), Laporan Hasil Monitoring. Jakarta. https://www.idsirtii.or.id/halaman/tentang/laporan-hasil-monitoring.html (accessed 26 September 2024).

National Cyber Security Agency (NACSA) (n.d), National Cyber Crisis Management Plan (NCCMP). https://www.nacsa.gov.my/nccmp.php (accessed 4 September 2024).

National Cyber Security Agency (NCSA) (2023), Annual Report 2023 (**รายงานประจำปี สกมช.** 2566). https://ncsa.or.th/Ebook_%E0%B8%A3%E0%B8%B2%E0%B8%A2%E0%B8%87%E0%B8%B2%E0%B8%99%20%E0%B8%AA%E0%B8%81%E0%B8%A1%E0%B8%8A/%E0%B8%A3%E0%B8%B2%E0%B8%A2%E0%B8%87%E0%B8%B2%E0%B8%99%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%88%E0%B8%B3%E0%B8%9B%E0%B8%B5%20%E0%B8%AA%E0%B8%81%E0%B8%A1%E0%B8%8A%202566.html? (accessed 5 September 2024).

National Electronics and Computer Technology Center (NECTEC) (n.d), Research. https://www.nectec.or.th/en/research (accessed 5 September 2024).

National Institute of Standards and Technology (2024), The NIST Cybersecurity Framework (CSF) 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (accessed 20 August 2024).

National Security Council, Malaysia (2020), Malaysia Cyber Security Strategy 2020-2024. https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf (accessed 4 September 2024).

National Security Council, Philippines (2023), National Security Policy Manual 2023-2028. https://nsc.gov.ph/images/NSS_NSP/National_Security_Policy_Manual_FINAL_E-COPY_with_WATERMARK_140823.pdf (accessed 31 July 2024).

Navigant Research (2018), Distributed Energy Resources Management Systems - Defining DERMS Use Cases and Value Propositions. https://plma.memberclicks.net/assets/resources/Navigant%20Research%20-%20AutoGrid%20DERMS%20White%20Paper.pdf (accessed 27 July 2024).

NISC (n.d.), About NISC. https://www.nisc.go.jp/eng/index.html (accessed 24 August 2024).

North American Electric Reliability Corporation (2024), About NERC. Washington, DC. https://www.nerc.com/AboutNERC/Pages/default.aspx (accessed 20 August 2024).

North American Electric Reliability Corporation (2024), Electricity Information Sharing and Analysis Center. Washington, DC.

https://www.nerc.com/pa/CI/ESISAC/pages/default.aspx (accessed 20 August 2024).

Norton Rose Fulbright (2019), Renewable energy snapshot: Myanmar. Singapore. https://www.nortonrosefulbright.com/en-us/knowledge/publications/d63c2e71/renewable-energy-snapshot-myanmar (accessed 30 July 2024).

OpenDevelopment Cambodia (2017), Electricity Infrastructure. Cambodia. https://opendevelopmentcambodia.net/topics/electricity-infrastructure (accessed 29 July 2024).

OpenDevelopment Cambodia (2023), Foreign Investors. Cambodia. https://opendevelopmentcambodia.net/topics/foreign-investors/ (accessed 29 July 2024).

OpenGovAsia (2023), Indonesia and UK Strengthen Cybersecurity Cooperation. Jakarta. https://opengovasia.com/2023/06/30/indonesia-and-uk-strengthen-cybersecurity-cooperation/ (accessed 20 August 2024).

People's Public Security Newspaper (2020), Department of Cyber Security and Hi-tech Crime Prevention Requested to Effectively Prevent Cyber Crimes. https://en.cand.com.vn/public-security-forces/Department-of-Cyber-Security-and-Hi-tech-Crime-Prevention-requested-to-effectively-prevent-cyber-crimes-i549548/ (accessed 9 September 2024).

Philippine Electricity Market Corporation (2024), Annual Market Assessment Report. Philippines. https://www.wesm.ph/downloads/download/TWFya2V0IFJlcG9ydHM=/MzIyNg== (accessed 1 August 2024).

Philippine Electricity Market Corporation (n.d.), Market Development - Retail. Philippines. https://www.wesm.ph/market-development/retail (accessed 1 August 2024).

PLN (2020), Pengembangan Smart Grid di Indonesia. Indonesia. https://iea.blob.core.windows.net/assets/8409fbba-7c53-4c95-89c2-3f653fd4ffd7/210226SmartGridsWS-PLNpresentation.pdf (accessed 27 August 2024).

PLN (2022), Dukung Transformasi Digital, PLN dan BSSN Perkuat Pembentukan Tim Tanggap Insiden Siber Pertama di Sektor Energi. Jakarta. https://web.pln.co.id/cms/media/2022/07/dukung-transformasi-digital-pln-dan-bssn-perkuat-pembentukan-tim-tanggap-insiden-siber-pertama-di-sektor-energi/ (accessed 12 September 2024).

PLN (2024), Penetapan-Tariff-Adjustment-Juli-September-2024. Indonesia. https://web.pln.co.id/statics/uploads/2024/07/Penetapan-Tariff-Adjustment-Juli-September-2024.jpg (accessed 23 August 2024).

Power Philippines (2021), USAID sets aside Php1.6B for clean energy projects. https://powerphilippines.com/usaid-sets-aside-php1-6b-for-clean-energy-projects/ (accessed 2 August 2024).

Prime Minister of Australia (2023), Joint Declaration on a Strategic Partnership between the Republic of the Philippines and the Commonwealth of Australia.

https://www.pm.gov.au/media/joint-declaration-strategic-partnership-between-republic-philippines-and-commonwealth (accessed 2 August 2024).

Professor Pawee Jenweeranon (n.d), Thailand's Cyber Resilience Journey: Understanding Obstacles and Uncovering Remedies. https://techforgoodinstitute.org/blog/expert-opinion/thailands-cyber-resilience-journey-understanding-obstacles-and-uncovering-remedies/ (accessed 5 September 2024).

PV Magazine (2020), Indonesia's first PPA for large scale solar. https://www.pv-magazine.com/2020/03/04/indonesias-first-ppa-for-large-scale-solar/ (accessed 23 August 2024).

PV Magazine (2024), Indonesian government abolishes net metering. https://www.pv-magazine.com/2024/02/28/indonesian-government-abolishes-net-metering/ (accessed 22 August 2024).

PV Magazine (2024), Vietnam sets $0.026/kWh tariff for net-metered solar power. https://www.pv-magazine.com/2024/07/16/vietnam-sets-0-026-kwh-tariff-for-net-metered-solar-power/ (accessed 6 September 2024).

Renewable Energy Magazine (2018), Sunseap Signs 21-Year Deal with PSA Singapore. https://www.renewableenergymagazine.com/pv_solar/sunseap-signs-21year-deal-with-psa-singapore-20180117 (accessed 31 July 2024).

Resecurity (2023), Ransomware Attacks against the Energy Sector on the rise - Nuclear and Oil & Gas are Major Targets in 2024. https://www.resecurity.com/blog/article/ransomware-attacks-against-the-energy-sector-on-the-rise-nuclear-and-oil-gas-are-major-targets-2024 (accessed 5 September 2024).

Reuters (2023), Indonesia's president launches carbon emissions credit trading. https://www.reuters.com/sustainability/sustainable-finance-reporting/indonesias-president-launches-carbon-emissions-trading-2023-09-26/ (accessed 26 August 2024).

ScienceDirect (2021), Malaysia's electricity market structure in transition. https://www.sciencedirect.com/science/article/abs/pii/S0957178721001004 (accessed 5 August 2024).

SEA information Platform for the Energy Transition (n.d.), Indonesia Power Sector Snapshot. https://www.sipet.org/power-sector-snapshot-indonesia.aspx (accessed 19 August 2024).

SEA information Platform for the Energy Transition (n.d.), Vietnam Power Sector Snapshot. https://www.sipet.org/power-sector-snapshot-vietnam.aspx (accessed 2 September 2024).

SGDSN (n.d.), SGDSN in English. https://www.sgdsn.gouv.fr/sgdsn-english (accessed 22 August 2024).

Singapore Statutes Online (2020), Electricity Act 2001. Singapore. https://sso.agc.gov.sg/act/ea2001 (accessed 30 July 2024).

Smart Energy International (2023), EGAT advances Thailand's smart grid development. https://www.smart-energy.com/industry-sectors/energy-grid-

management/egat-advances-thailands-smart-grid-development/ (accessed 16 August 2024).

SoyaCincau (2024), Go To-U claims R00tk1t compromised TNB Electron app, affecting TNBX. https://soyacincau.com/2024/02/19/go-to-u-claims-r00tk1t-tnb-electron-tnbx/ (accessed 4 September 2024).

SP Power Group (2011), Annual Report. Singapore. https://www.spgroup.com.sg/dam/spgroup/pdf/annual-reports/SP-Group-Annual-Report-FY1011.pdf (accessed 30 July 2024).

Statista (2024), Annual number of cyberattacks in the United States from 2016 to 2022. https://www.statista.com/forecasts/1448523/us-cyberattacks-annual (accessed 21 August 2024).

Statista (2024), Number of cleared cybercrime cases in Japan from 2014 to 2023. https://www.statista.com/statistics/746963/japan-number-of-cyber-crime-arrests/ (accessed 24 August 2024).

Statista (2024), Number of cybercrime reports made to the Australian Cyber Security Centre in Australia from financial year 2020 to financial year 2023. https://www.statista.com/statistics/1343645/australia-number-of-cybercrimes-reports-acsc/ (accessed 23 August 2024).

Statista (2024), Number of incidents of data breaches in the Philippines from 1st quarter 2020 to 4th quarter 2023. https://www.statista.com/statistics/1271333/philippines-number-of-data-breaches/ (accessed 30 July 2024).

Statista (2024), Number of mobile malware attacks detected in the Philippines from 2019 to 2022. https://www.statista.com/statistics/1277044/philippines-number-of-foiled-mobile-malware/ (accessed 30 July 2024).

Suruhanjaya Tenaga Energy Commission (2023), Information Guide For Corporate Green Power Programme. Malaysia. https://www.st.gov.my/en/contents/files/download/154/Guide_CGPP-_31_Jan_2023.pdf (accessed 7 August 2024).

Sustainable Energy Development Authority Malaysia (n.d.), Net Energy Metering (NEM) 2.0. Malaysia. https://www.seda.gov.my/reportal/nem2/ (accessed 6 August 2024).

Sustainable Energy Development Authority Malaysia (n.d.), Net Energy Metering (NEM) 3.0. Malaysia. https://www.seda.gov.my/reportal/nem/ (accessed 6 August 2024).

Tech2Thai (n.d), Six months of phishing attacks in 2022 exceed SEA's total number last year. https://www.tech2thai.com/enterprise_tech/1990/six-months-of-phishing-attacks-in-2022-exceed-sea-rsquo-s-total-number-last-year (accessed 3 August 2024).

Tenaga Nasional Berhad (n.d.), Frequently Asked Questions. Malaysia. https://www.mytnb.com.my/faq (accessed 7 August 2024).

Tenaga Nasional Berhad (TNB) (n.d), About TNB. https://www.tnb.com.my/about-tnb (accessed 4 September 2024).

Tenaga Nasional Berhad (TNB) (n.d), Smart Grid. https://www.tnb.com.my/smart-grid/ (accessed 4 September 2024).

Thai Computer Emergency Response Team (ThaiCERT) (n.d), About NCERT. https://www.thaicert.or.th/en/about-ncert/ (accessed 5 September 2024).

Thailand Board of Investment (2023), Investment Promotion Guide. Thailand. https://www.boi.go.th/upload/content/BOI_A_Guide_EN.pdf (accessed 8 August 2024).

Thailand Board of Investment (2023), Thailand's Electricity Market. Thailand. https://www.boi.go.th/index.php?page=electricity (accessed 7 August 2024).

Thailand Development Research Institute (2023), Electricity liberalisation, the way of leading the country towards clean, affordable, and equitable electricity. Thailand. https://tdri.or.th/en/2023/11/electricity-liberalisation-the-way-of-leading-the-country-towards-clean-affordable-and-equitable-electricity/ (accessed 8 August 2024).

Thailand Greenhouse Gas Management Organisation (2023), Project Specifications - Project Type. Thailand. https://tver.tgo.or.th/index.php/en/en-standard/kar-phathna-khorngkar-en/khx-kahnd-khorngkar-en/std-en-project-type (accessed 13 August 2024).

Thailand Greenhouse Gas Management Organisation (n.d.), Overview. Thailand. https://tver.tgo.or.th/index.php/en/en-about/en-overview (accessed 13 August 2024).

Thailand Greenhouse Gas Management Organisation (n.d.), Voluntary carbon credit prices in Thailand. Thailand. https://carbonmarket.tgo.or.th/index.php?lang=TH&mod=Y2N0X3ByaWNl (accessed 13 August 2024).

The Cyber Express (2024), MIDF cyberattack claims by Rhysida. https://thecyberexpress.com/midf-cyberattack-claims-by-rhysida/ (accessed 3 August 2024).

The Diplomat (2018), What's Behind Vietnam's New Military Cyber Command?. https://thediplomat.com/2018/01/whats-behind-vietnams-new-military-cyber-command/ (accessed 9 September 2024).

The International Tracking Standard Foundation (2022), Brunei approved for I-REC(E) issuance. https://www.trackingstandard.org/brunei-approved-for-i-rece-issuance/ (accessed 8 August 2024).

The Laotian Times (2024), Laos Launches Forest Carbon Credit Initiative to Combat Climate Change. Lao PDR. https://laotiantimes.com/2024/05/09/laos-launches-forest-carbon-credit-initiative-to-combat-climate-change (accessed 19 August 2024).

The Star (2023), Cybersecurity report ranks Malaysia as eighth most breached country in Q3 2023. https://www.thestar.com.my/tech/tech-news/2023/12/06/cybersecurity-report-ranks-malaysia-as-eighth-most-breached-country-in-q3-2023 (accessed 3 August 2024).

The Straits Times (2017), Personal data of 850 national servicemen and Mindef staff stolen in targeted cyber attack. https://www.straitstimes.com/singapore/personal-data-of-850-mindef-servicemen-and-staff-leaked-due-targeted-planned-cyber-attack (accessed 3 October 2024).

Tilleke & Gibbins (2020), Thailand Issues Regulations for Procurement of Electricity from Very Small Power Plants. https://www.tilleke.com/insights/thailand-issues-regulations-procurement-electricity-very-small-power-plants/3/ (accessed 13 August 2024).

Today Singapore (2023), Cyberattack caused 7-hour internet outage that hit public hospitals, polyclinics; attacks continuing: Synapxe. https://www.todayonline.com/singapore/cyberattack-caused-7-hour-internet-outage-hit-public-hospitals-polyclinics-attacks-continuing-synapxe-2297036 (accessed 3 October 2024).

Tripwire (2024), IoT Security Regulations: A Compliance Checklist – Part 1. https://www.tripwire.com/state-of-security/iot-security-regulations-compliance-checklist-part-1 (accessed 18 September 2024).

Tuoi Tre News (2024), Petrovietnam Oil Corp hit by ransomware attack. https://tuoitrenews.vn/news/business/20240403/petrovietnam-oil-corp-hit-by-ransomware-attack/79151.html (accessed 5 September 2024).

U.S. Mission to ASEAN (n.d), USAID ASEAN. https://asean.usmission.gov/usaidasean/ (accessed 5 September 2024).

Urban LEDS (2021), Lao Cities Pursue Low-Carbon Development with Solar Power and Energy Efficiency Projects. Lao PDR. https://urban-leds.org/lao-cities-pursue-low-carbon-development-with-solar-power-and-energy-efficiency-projects/ (accessed 29 July 2024).

US Congress (2020), H.R.1668 - IoT Cybersecurity Improvement Act of 2020. https://www.congress.gov/bill/116th-congress/house-bill/1668 (accessed 21 August 2024).

US Department of Energy (2021), Cybersecurity Risk Information Sharing Program (CRISP). Washington, DC. https://www.energy.gov/sites/default/files/2021-12/CRISP%20Fact%20Sheet_508.pdf (accessed 20 August 2024).

US Department of Energy (2024), Cybersecurity Research, Development, and Demonstration (RD&D) for Energy Delivery Systems. Washington, DC. https://www.energy.gov/ceser/cybersecurity-research-development-and-demonstration-rdd-energy-delivery-systems (accessed 21 August 2024).

US Department of Energy (2024), Office of Cybersecurity, Energy Security, and Emergency Response - Authorities and Roles. Washington, DC. https://www.energy.gov/ceser/authorities-and-roles (accessed 20 August 2024).

US Department of Homeland Security (2024), About CISA. https://www.dhs.gov/keywords/cybersecurity-and-infrastructure-security-agency-cisa (accessed 20 August 2024).

US Department of State (2020), 2020 Investment Climate Statements: Brunei. Washington, DC. https://www.state.gov/reports/2020-investment-climate-statements/brunei (accessed 19 September 2024).

USAID (2022), USAID supports Vietnam's innovation and digital transformation in the public sector. https://www.usaid.gov/vietnam/news/apr-8-2022-usaid-supports-vietnams-innovation-and-digital-transformation-public-sector (accessed 9 September 2024).

Vietnam Briefing (2019), Renewables in Vietnam: Current Opportunities and Future Outlook. https://www.vietnam-briefing.com/doing-business-guide/vietnam/sector-insights/industry-spotlight-vietnam-s-renewable-energy-market (accessed 3 September 2024).

Vietnam Briefing (2024), Vietnam's Digital Infrastructure Master Plan to 2030: Roadmap to a High-Tech Future. https://www.vietnam-briefing.com/news/vietnams-digital-infrastructure-master-plan-2030-roadmap-to-a-high-tech-future.html/ (accessed 9 September 2024).

Vietnam Information Security Association (VNISA) (n.d), About VNISA. https://vnisa.org.vn/en/about-vnisa/ (accessed 9 September 2024).

Vietnam Information Security Association (VNISA) (n.d), Cybersecurity Emergency Response Center established. https://vnisa.org.vn/en/cybersecurity-emergency-response-center-established/ (accessed 5 September 2024).

Vietnam News (2016), Chinese hackers attack VN's airports and Vietnam Airlines' website. https://vietnamnews.vn/society/300416/chinese-hackers-attack-vns-airports-and-vietnam-airlines-website.html (accessed 5 September 2024).

World Bank (n.d.), Accessibility to electricity in rural (% of rural population). https://data.worldbank.org/indicator/EG.ELC.ACCS.RU.ZS (accessed 29 July 2024).

Appendix

1-1. Electricity Business Environment in each ASEAN Country

1-1-1. Singapore

(1) Market Structure

Singapore's energy market is highly liberalised and has been restructured to promote competitive, secure and reliable supply of electricity.

Overview of the Electricity System in Singapore[33,34,35]

Regulatory Body:

- The Energy Market Authority (EMA) was established in 2001 following the liberalisation of the energy industry to regulate the electricity and gas markets and ensure the stability of the electricity system.
- It is legal organisation under the Ministry of Trade and Industry (A legal entity established under an individual law that regulates the relationship between the statutory body and the ministry. Staff are not public servants).
- Its roles and responsibilities are to implement electricity, city gas and district heat supply regulations and issues licenses to companies involved in the electricity, gas and district cooling sectors.

Generation:

- The generation base (total 54.6TWh) as of 2022 consists of majority of Gas (91%), Coal (1%), Oil (0.4%) and Others – Petroleum Products and Renewable Energy (7.6%). Singapore has small land area and poor renewable energy potential. Most of primary energy depends on imports.
- Power companies have a 91% capacity share with 9% from home generation. There is licenced for 18 entities and the main players as of 2022 are Senoko Energy (2.8GW), YTL Power Seraya (2.4GW), Tuas Power Generation (2.0GW), Keppel Merlimau Cogen (1.3GW), SembCorp Cogen (1.4GW), PacificLight Power (0.8GW) and Taser Power (0.4GW).

---

[33] Energy Market Authority (2024), Energy Market Landscape. Singapore. https://www.ema.gov.sg/our-energy-story/energy-market-landscape/electricity (accessed 30 July 2024).

[34] SP Power Group (2011), Annual Report. Singapore. https://www.spgroup.com.sg/dam/spgroup/pdf/annual-reports/SP-Group-Annual-Report-FY1011.pdf (accessed 30 July 2024).

[35] Energy Market Company (2024), NEMS Market Report 2023. Singapore. https://www.home.emcsg.com/publications/-/media/Comms/NEMS-Market-Reports/NEMS-Market-Report-2023_Final_3.pdf (accessed 30 July 2024).

Transmission / Distribution:

- SP PowerGrid operates facilities owned by SP PowerAssets. SP PowerAssets (under SP Group) is the only transmission licensee.
- Grid operators are PSOs (a division of EMA).
- Standard voltage of 66kV–400kV.
- SP PowerAssets owns transmission and distribution equipment, including 12,000 substations, a 29,000km underground line; Power Gas (also under SP Group) own transmission and distribution assets including 2,800km of pipelines
- There are no embedded networks or distribution policy to support any distribution exemption such as in industrial parks and shopping malls.

Trading Market:

- Through the National Electricity Market of Singapore (NEMS) which consists of a spot market and a reserve electricity market and is operated by The Energy Market Company Pte Ltd.
- Market participants can choose to procure from (1) the spot market, (2) procure through bilateral contracts, or (3) procure at regulated prices through SP Services.
- There are a total of 100 market participants (based on EMA licenses): 18 power generation companies, 19 retailers, 63 wholesalers.

Retail:

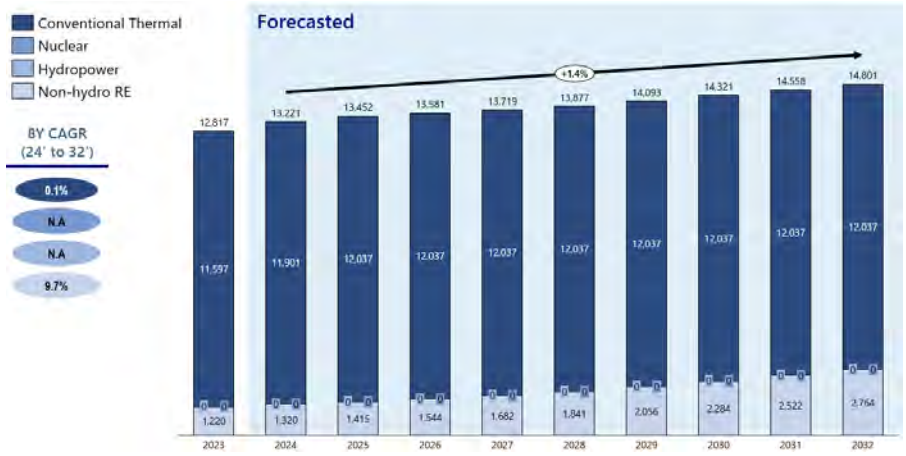
- Fully liberalised since Nov 2018. Licenced to 19 companies as of 2022 with 90.9% share by six big players. The main players as of 2022 are: SP Services (25.9%), Tuas Power Supply (19.2%), Seraya Energy (13.5%), Senoko Energy Supply (13.1%), Keppel Electric (9.8%), SembCorp Power (9.4%) and PacificLight Energy (7.2%).
- SP Group, which has been supplying power to non-liberalised customers, continues to supply power at regulated rates. Consumers can still choose SP Group.

100% FDI is allowed for electricity sector (including power generations) in Singapore since 2001 and there are no specific restrictions on foreign ownership of electricity companies or assets (be it renewable or not). However, there are restrictions on shareholding which apply generally to any ownership of designated electricity licensees, designated entities and designated business trusts: 'Designated electricity licensees, designated entities and the trustee-manager of a designated business trust must give notice to the Energy Market Authority (EMA) if any entity acquires an equity interest in the licensee, entity or business trust that would result in them holding between 5% but less than 12% of the total equity

interest in that licensee, entity or business trust' (section 30B, Electricity Act)[36].

Singapore's energy capacity is projected to increase at a CAGR of 1.4% to 14,801MW in 2032. Majority of the energy mix comes from conventional thermal.

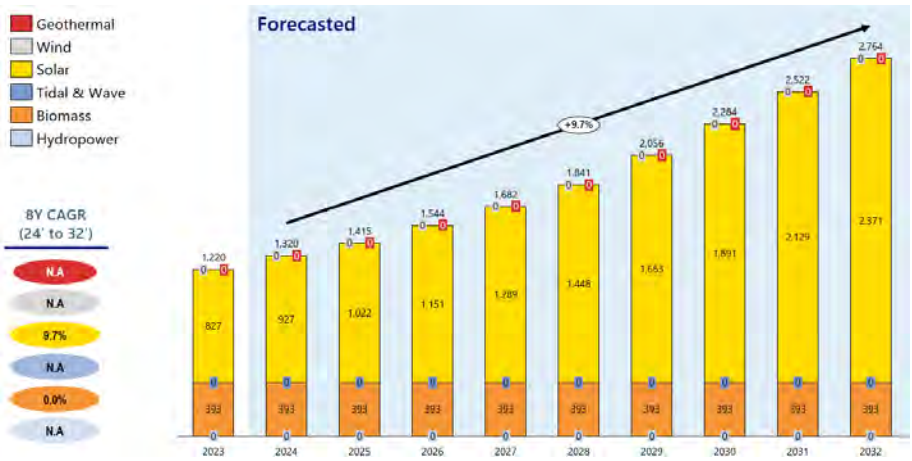
Figure A.1 Total Energy Mix Capacity (MW, 2023-2032F)



Source: Created by authors based on Fitch Solutions.

For renewable energy, most comes from solar power, which is also the fastest growing segment at 9.7% CAGR.

Figure A.2 Renewable Energy Mix Capacity (MW, 2023-2032F)



Source: Created by authors based on Fitch Solutions.

(2) Bilateral Trading

In Singapore, the Net-Metering scheme is an incentive mechanism that defines different methods of pricing the sale of surplus electricity depending on the type of customer. SP Group customers use the Simplified Credit Treatment (SCT) scheme, while others use the Enhanced Central Intermediary (ECI) scheme, with surplus electricity paid at the regulated price plus grid charge (approx. 6 cents/kWh) in the former case, and at the wholesale

[36] Singapore Statutes Online (2020), Electricity Act 2001. Singapore. https://sso.agc.gov.sg/act/ea2001 (accessed 30 July 2024).

electricity market price in the latter case[37].

SCT Scheme

- Eligibility: Only applicable to non-contestable consumers and residential solar panel installations < 1 MWac capacity.
- Mechanism: Non-contestable consumers that sell excess energy to the market will be paid at the prevailing tariff minus grid charges. SCT compensates consumers for any surplus energy that solar panels generate at the prevailing tariff rates, deducting grid charges.

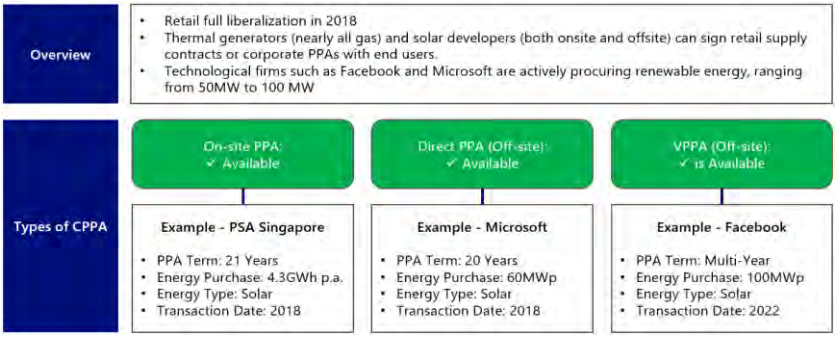
ECI Scheme

- Eligibility: Applicable to both residential and commercial solar installations and applicable to contestable consumers and solar panel installations with < 10 MWac capacity.
- Mechanism: Under this scheme, contestable consumers that sell any excess energy to the market will receive payment based on the prevailing half-hourly wholesale electricity prices.

Other than the net-metering scheme, customers can participate in CPPAs which has been available in Singapore since 2018.

[37] Energy Market Authority (2024), Solar - Solar Installation Guide. Singapore. https://www.ema.gov.sg/consumer-information/solar/solar-installation-guide (accessed 31 July 2024).

Figure A.3 CPPA Schemes in Singapore



Source: Created by authors based on Bird & Bird[38], Data Center Dynamics[39], Microsoft[40] and Renewable Energy Magazine[41]

The existence of technological giants in Singapore plays a big role for the uptake of CPPAs.

(3) Electricity Market Condition

In Singapore, there are wholesale market, Capacity market, voluntary carbon credit market and demand response programmes.

①Wholesale market

All of Singapore's electricity is bought and sold through Energy Market Company (EMC) in the National Electricity Market of Singapore (NEMS). EMC is the exchange for wholesale electricity trading, providing a transparent and competitive trading platform and the governance for the market.

Prices in the wholesale market (inclusive of ancillary services) experienced a broad decline across all categories from 2022 to 2023 but remain elevated and have been on an increase since 2019.

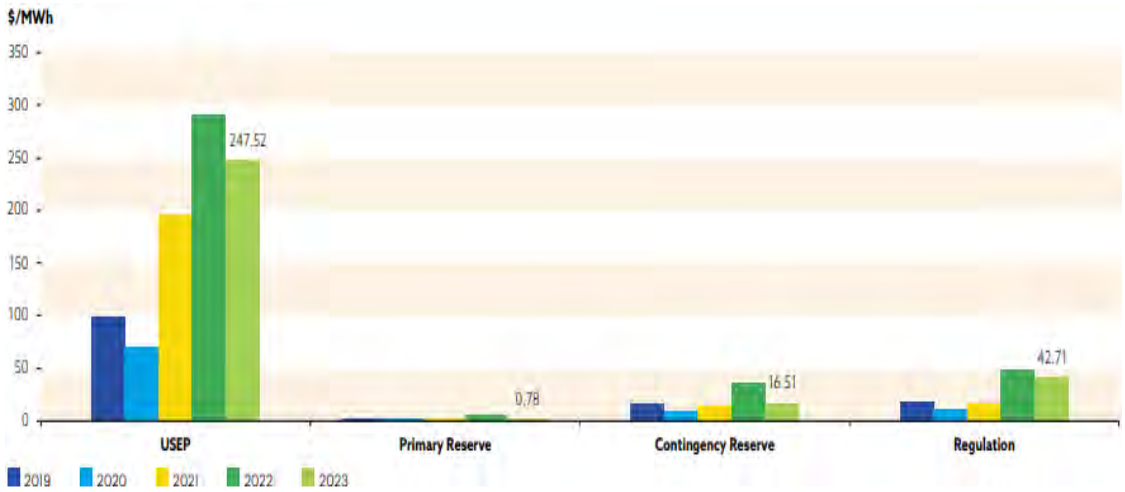
[38] Bird & Bird (2024), Solar Energy & Corporate PPAs in Singapore. https://www.twobirds.com/en/insights/2024/singapore/solar-energy-corporate-ppas-in-singapore (accessed 31 July 2024).

[39] Data Center Dynamics (2021), Facebook to buy renewable energy from offshore floating solar farm in Singapore. https://www.datacenterdynamics.com/en/news/facebook-to-buy-renewable-energy-from-offshore-floating-solar-farm-in-singapore/ (accessed 31 July 2024).

[40] Microsoft (2018), Microsoft and Sunseap sign agreement on largest-ever solar project in Singapore. https://news.microsoft.com/2018/02/28/microsoft-and-sunseap-sign-agreement-on-largest-ever-solar-project-in-singapore/ (accessed 31 July 2024).

[41] Renewable Energy Magazine (2018), Sunseap Signs 21-Year Deal With PSA Singapore. https://www.renewableenergymagazine.com/pv_solar/sunseap-signs-21year-deal-with-psa-singapore-20180117 (accessed 31 July 2024).

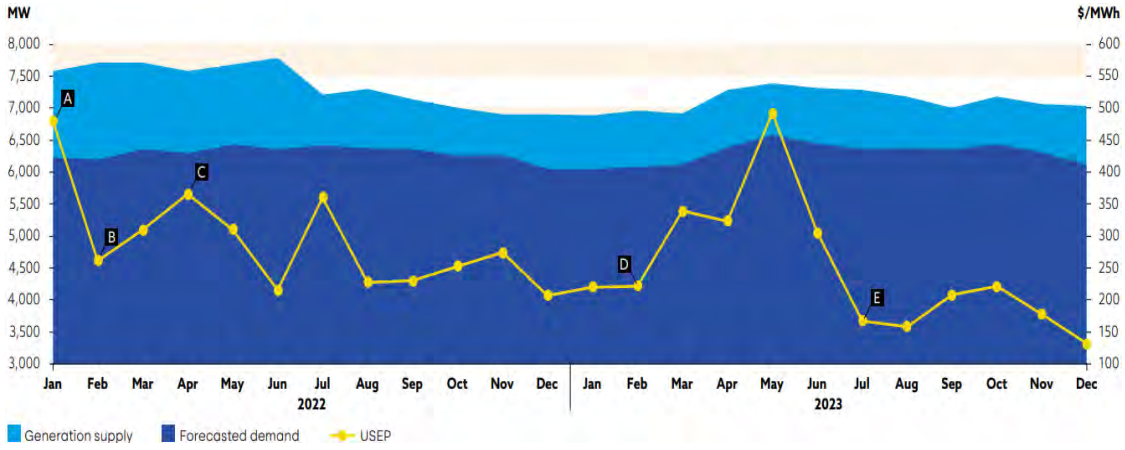
Figure A.4 Annual USEP and Ancillary Prices ($/MWh)



Source: Energy Market Company, 2024[42]

USEP Forecasted Demand and Generation Supply are steadily transiting between around 7,000MW and 6,000MW respectively, meaning the market rarely face the lack of electricity, while the market price range stabilised after introduction of Temporary price cap (TCP) mechanism to lower price from the second half of 2023.

Figure A.5 USEP Forecasted Demand and Generation Supply (2022–2023)



Source: Energy Market Company, 2024[43].

Volatile prices arising from the global energy crunch marked the beginning of 2022. To stabilise the market, the EMA introduced measures to help the market tide over the energy crunch such as the TPC mechanism which mitigates prolonged extreme price volatility by putting a temporary price cap on wholesale electricity prices, while the new Vesting

[42] Energy Market Company (2024), NEMS Market Report 2023. Singapore. https://www.home.emcsg.com/publications/-/media/Comms/NEMS-Market-Reports/NEMS-Market-Report-2023_Final_3.pdf (accessed 30 July 2024).

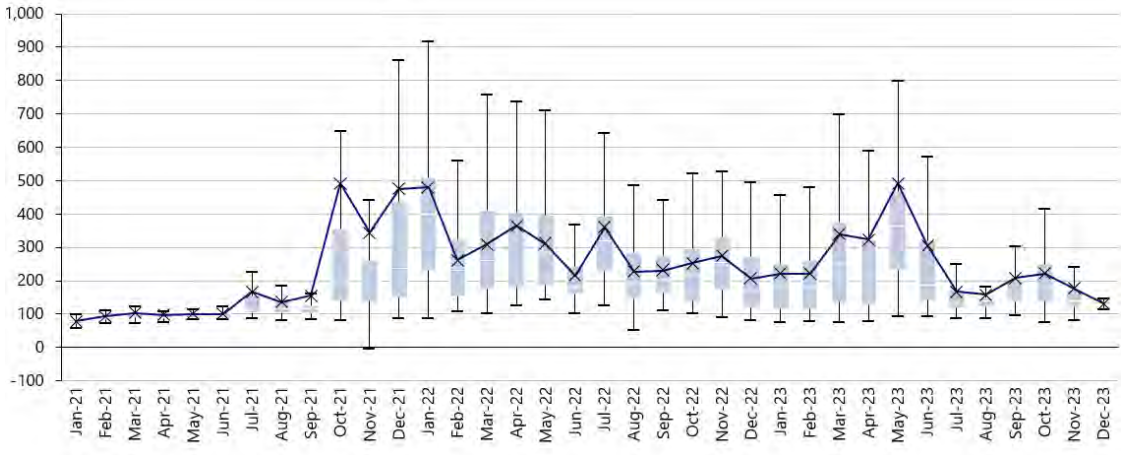
[43] Energy Market Company (2024), NEMS Market Report 2023. Singapore. https://www.home.emcsg.com/publications/-/media/Comms/NEMS-Market-Reports/NEMS-Market-Report-2023_Final_3.pdf (accessed 30 July 2024).

Regime Framework enables the Market Support Services Licensee (MSSL) to continue offering stable and regulated tariffs to non-contestable consumers.

The USEP averaged $318.84/MWh and $177.37/MWh in the first and second half of the year respectively. Compared to the first half of the year, the coefficient of variance of USEP fell 17.1% in the second half. This indicates that the USEP became less volatile in the second half of 2023 after the implementation of the TPC mechanism and new vesting regime.

Electricity price is typically established through the NEMS, where electricity generators (Gencos) and retailers participate. Gencos offer every half-hour to sell the electricity into the spot market for matching with the prevailing electricity demand at that period. The spot prices fluctuate markedly, during periods of tight supply due to plant outages or network constraints. The wholesale market is operated by EMC with around 24 wholesalers.

Figure A.6 Price Trend of Wholesale Market



Source: Created by authors based on Energy Market Company[44]

The wholesale market is subject to constant price fluctuations, with prices usually ranging around 40 SGD/MWh to 300 SGD/MWh during non-peak to peak periods.

②Ancillary Market

In the NEMS, two reserve products are traded: primary and contingency reserves. Each reserve has its own price and response time.

[44] Energy Market Company (2024), NEMS Market Report 2023. Singapore. https://www.home.emcsg.com/publications/-/media/Comms/NEMS-Market-Reports/NEMS-Market-Report-2023_Final_3.pdf (accessed 30 July 2024).

Table A.1 Overview of Ancillary Services Market

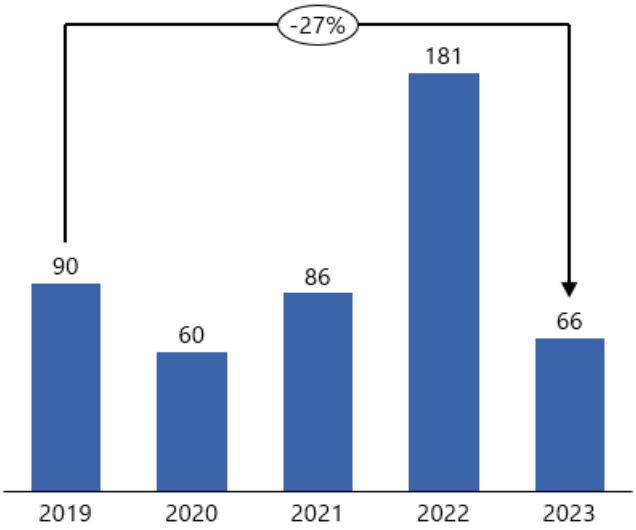
Market		Response time	Duration	Minimum load (for participation)	Contracted load	Aggregator participation	Participating aggregators
Ancillary	**Primary reserve** via Interruptible Load scheme	9 seconds	At least 30 minutes, up to 2.5 hours or more	0.1MW	1,347 MW (2023)	Yes	Diamond Energy Just Electric Enel X
	Contingency reserve via Interruptible Load scheme	10 minutes		0.1MW	3,671MW (2023)	Yes	
Energy	**DRP: Demand Response Programme**	Immediate	At least 30 minutes	0.1MW	5 facilities	Yes	Just Electric

Source: Created by authors based on Energy Market Company[45]

In the Interruptible Load programme, consumers can be paid to be on standby for their load to be shed in response to system contingency events. In the DRP: Demand Response programme, consumers can receive a share of the system-wide savings that result from demand response by reducing their electricity consumption during periods of high energy prices.

Compared to 2022, which recorded the highest reserve payment since the market started, reserve costs decreased 63.5% to $66.0 million. This was primarily driven by declines in both contingency reserve prices and the contingency reserve requirement.

Figure A.7 Annual Reserve Payment (2019-2023)



Source: Created by authors based on Energy Market Company[46]

[45] Energy Market Company (2024), NEMS Market Report 2023. Singapore. https://www.home.emcsg.com/publications/-/media/Comms/NEMS-Market-Reports/NEMS-Market-Report-2023_Final_3.pdf (accessed 30 July 2024).

[46] Energy Market Company (2024), NEMS Market Report 2023. Singapore. https://www.home.emcsg.com/publications/-/media/Comms/NEMS-Market-Reports/NEMS-Market-Report-2023_Final_3.pdf (accessed 30 July 2024).

In 2019, the total ancillary market is estimated to be USD60 million with interruptible load payments comprising about 2% of the reserve market share while the majority (approx. 98%) are reserve payments.

As of 31 December 2023, there was no registered capacity for interruptible load (IL) for primary reserve. For contingency reserve, the total IL registered capacity remained at 24.9MW. The number of IL activations for contingency reserve increased to 23 from 13, while the total number of periods when IL was activated for contingency reserve increased to 28 from 27 when compared to 2022.

To approximate for the ancillary market size in 2023, the total market size is likely to decrease as it has experience 27% decrease in reserve payments when compared to 2019.

③Carbon Credit Market

Singapore's carbon credit market size is projected to increase from USD14.5 million in 2023 to USD55.14 million in 2030 driven by a backdrop of environmental sustainability initiatives to advance its carbon neutrality and be the mainstream market of carbon credit trading in ASEAN. Based on the above, the market is forecasted to achieve CAGR of 21% from 2023 to 2030[47].

This change is driven by the following factors:

- In 2023, the government has rolled out the Eligibility Criteria under the International Carbon Credit (ICC) Framework. This provides regulatory clarity as Singapore positions itself as an international carbon market which acts as a boost to its carbon credit market size as Singapore progresses in achieving net zero emissions by 2050.
- There are currently more than 70 carbon services and trading firms that use Singapore as a base to serve the region and engage in carbon market activities and this ecosystem effect is expected to attract further participation by market players.

Singapore aims to create a robust carbon trading ecosystem with strong support from the government for a viable trading environment.

[47] Coherent Market Insights (2024), Singapore's Carbon Credit Market Surging At 21% CAGR. https://carboncredits.com/singapores-carbon-credit-market-surging-at-21-cagr/ (accessed 31 July 2024).

Table A.2 Carbon Credit Exchange Overview

	CIX (Climate Impact X)	ACX (Air Carbon Exchange)
Overview	▪ International online trading marketplace for trading voluntary carbon credits ▪ Established in May 2021 by four institutions: DBS Bank, Singapore Exchange (SGX), Standard Chartered Bank (UK) and Temasek Holdings, a Singapore government-owned investment company	▪ International online trading marketplace for trading voluntary carbon credits ▪ Established in 2019 by Thomas McMahon (former CEO and Managing Director of Singapore Mercantile Exchange) and others
Features	▪ Satellite monitoring, machine learning and blockchain technology to ensure transparency, consistency and high quality of carbon credits ▪ Forest-based credits expected to be tradable ▪ Two types of platforms offered (1) The Exchange ➢Trade packaged credits for multiple PJs (2) The Project Marketplace ➢Trading credits for specific projects.	▪ Manage tokenised credits (AirCarbon Token) on the blockchain and operate an exchange ▪ Trade a wide variety of credits (CORSIA standard, forest-derived, renewable energy-derived, etc.) ▪ Awarded "Best Carbon Exchange" in the 2021 Voluntary Carbon Market Rankings by Environmental Finance magazine.
Transaction results	▪ Pilot auction in October 2021 19 companies including BCG, DBS, ENGIE, TRAFIGURA and VITOL participate, trading 170,000 tonnes. ▪ Aim to start full-scale trading by the end of 2022	▪ In 2021, approximately 3.6 million tonnes were traded by the end of the second quarter of the year ▪ Credit prices as of June 2022 range from 2 to 11 USD/t (6-9 USD/t for forest-based credits) ▪ Trade by tech companies (Hong Kong BC Technology Group) and environmental start-ups (bioeconomy) is seen

Source: Created by authors based on CIX[48] and ACX[49]

The growth in carbon credit trading market will be facilitated by key carbon credit exchange players in Singapore such as CIX and ACX.

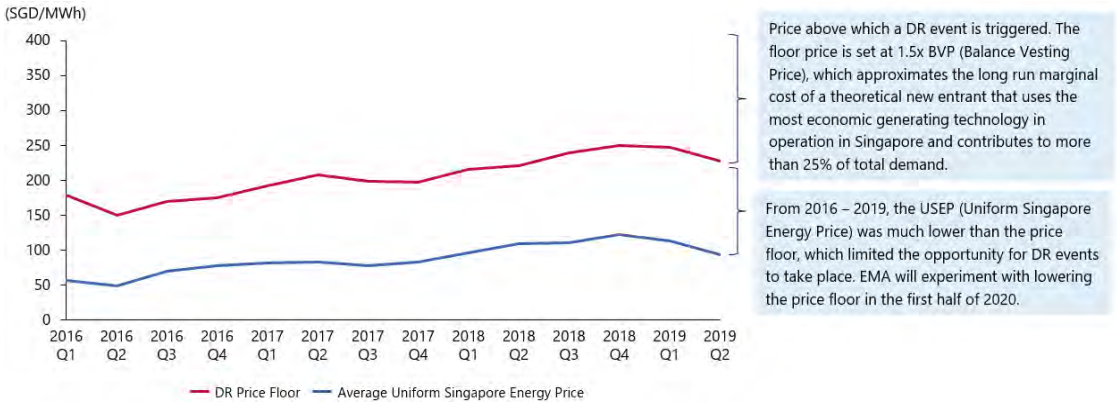
④Demand Response Programmes

The DR programme was introduced in 2016 to enable contestable consumers to participate directly in the wholesale market by reducing electricity demand voluntarily in response to market conditions. From 2016 to 2019, the marginal cost of generation did not exceed the existing DR Price Floor and participation in DR programmes has been limited and under–utilised since their introduction.

[48] Climate Impact X (n.d.), CIX Exchange. https://www.climateimpactx.com/exchange (accessed 1 August 2024).

[49] Air Carbon Exchange (n.d.), ACX Singapore. https://acx.net/acx-singapore/ (accessed 1 August 2024).

Figure A.8 DR Price Floor and USEP (2016–2019)

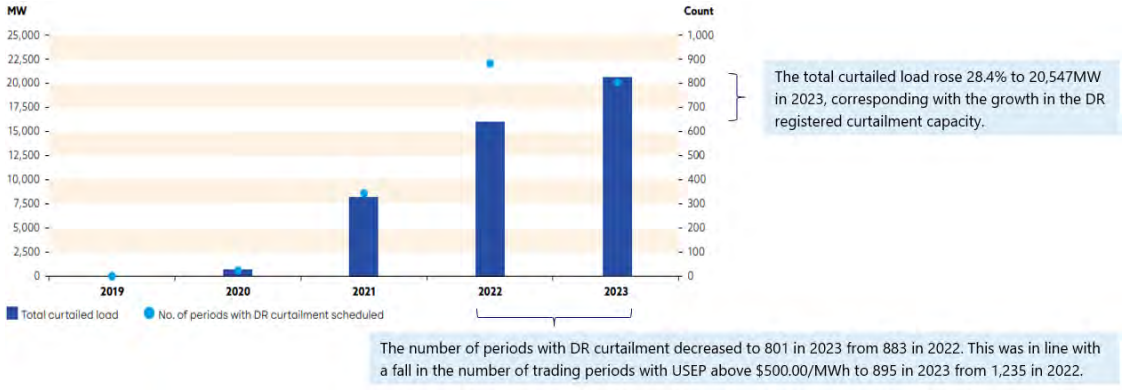


Source: Created by authors based on Energy Market Company[50]

There is currently only one registered DR load capacity of 7.2MW by Diamond Energy Merchants Pte Ltd. Since 2016, there have only been 2 instances of DR bids being dispatched. This is because the spot price of electricity rarely went above the floor price set by the EMA.

To encourage more participation in the DR programme, a Demand Side Management (DSM) Sandbox was introduced from 1 January 2023 to 31 December 2024[51]. During the sandbox period, the threshold for non-compliance is lowered from 95 to 80%. The penalty regime is further relaxed such that no penalties are incurred for the first two instances of under-delivery.

Figure A.9 Annual Demand Response Scheduled (2019-2023)



Source: Energy Market Company[52]

---

[50] Energy Market Company (2024), NEMS Market Report 2023. Singapore. https://www.home.emcsg.com/publications/-/media/Comms/NEMS-Market-Reports/NEMS-Market-Report-2023_Final_3.pdf (accessed 30 July 2024).

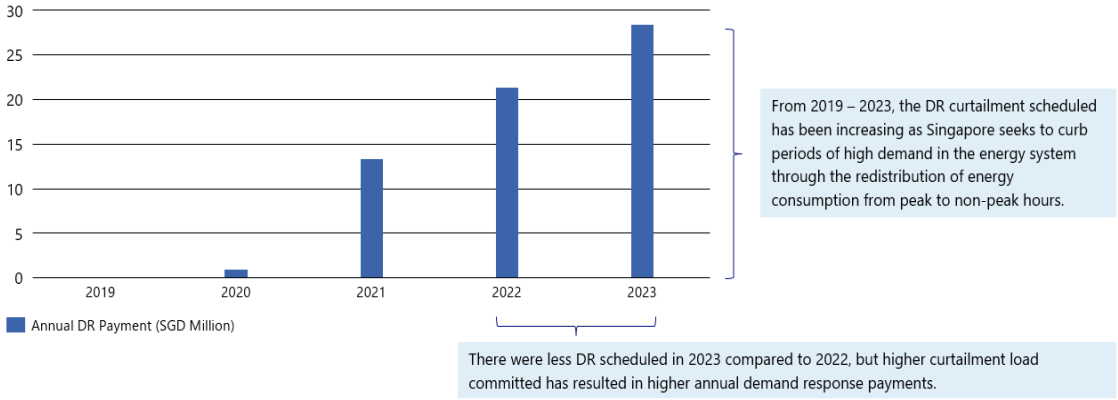
[51] Energy Market Authority (2022), Enhancing the Demand Response (DR) and Interruptible Load (IL) Programmes with a Demand Side Management Sandbox. Singapore. https://www.ema.gov.sg/content/dam/corporate/our-energy-story/energy-demand/factsheet-demand-response-interruptible-load_20221103.pdf (accessed 30 July 2024).

[52] Energy Market Company (2024), NEMS Market Report 2023. Singapore.

From 2019 to 2023, the rising cost of generation and enhancement to DR programmes through the DR sandbox by the energy authority has led to greater demand for DR.

Correspondingly, from 2019 to 2023, the annual DR payment has been on the rise in line with the higher frequency of DR curtailment scheduled.

Figure A.10 Annual Demand Response Payments (2019–2023)



Source: Created by authors based on Energy Market Company[53]

Average cost savings increases as the spread between USEP, and peak demand has widened in recent years. This spurs players to participate in DR as they can benefit from higher cost savings to help in reducing demand. However, it is unclear whether the trend on higher average cost savings will continue beyond 2024 as annual demand for DR scheduled has drop from 2022 to 2023, but 2023 still see higher annual DR payment as the total curtailed load was higher in 2023 compared to 2022 due to higher participation.

(4)Future Opportunities for DES

Singapore is unlikely to expand due to the current system-based limitation with generation overcapacity (as the peak supply capacity is about double its peak demand) and low electricity prices. The recent 3 years have been an anomaly due to Covid-19 and geopolitical conflict disrupting the cost of production for electricity. Moving forward, the focus in increasing demand for ancillary services through introduction of a 5-minute dispatch interval may lead to stabilisation of the grid, but it is not clear if or when such a system will be implemented in Singapore. The adoption of DES in Singapore will not be as attractive when compared to other ASEAN countries due to a lower need for such a solution.

https://www.home.emcsg.com/publications/-/media/Comms/NEMS-Market-Reports/NEMS-Market-Report-2023_Final_3.pdf (accessed 30 July 2024).

[53] Energy Market Company (2024), NEMS Market Report 2023. Singapore. https://www.home.emcsg.com/publications/-/media/Comms/NEMS-Market-Reports/NEMS-Market-Report-2023_Final_3.pdf (accessed 30 July 2024).

1-1-2.Philippines

(1)Market Structure

Philippines energy market is liberalised. Private participation is permitted in both the transmission and distribution business in Philippines.

Overview of the Electricity System in Philippines[54,55,56,57]

Regulatory Body:

- Established in 2001, the Energy Regulatory Commission (ERC) ensures the adequate promotion of consumer interests and customer choice; promotes competition, encourages market development, and penalises abuse of market power. It is also responsible for enforcing the implementing rules and regulations.

Generation:

- Installed capacity of 26,251 MW as of 2020 with heavy dependence on Coal (57.2%), Renewable Energy (21.2%), Natural Gas (19.2%) and Oil-based (2.4%).
- Power companies are divided into two patterns (1) IPP: Introduced from 1993 and the three conglomerate, San Miguel Energy, First Gen, Aboitiz Power occupy a high share and (2) National Power Corporation (NPC): Owns most power generation assets since its establishment in 1936.
- Market share and generation cap are in place to prevent market dominance.

Transmission / Distribution:

- The National Grid Corporation of the Philippines (NGCP), invested by State Grid Corporation of China, implements the transmission business. National Transmission Corporation (TRANSCO) provides supervision on asset ownership and business operation. The NGCP was transferred from TRANSCO in 2009.
- For distribution, Private PDU such as Meralco and Visayan Electric Company (VECO) and private distribution system operators (DSO) are major players.

---

[54] Independent Electricity Market Operator (n.d.), About the Philippine Electricity Market. Philippines. https://www.iemop.ph/the-market/ (accessed 1 August 2024).

[55] Philippine Electricity Market Corporation (2024), Annual Market Assessment Report. Philippines. https://www.wesm.ph/downloads/download/TWFya2V0IFJlcG9ydHM=/MzIyNg== (accessed 1 August 2024).

[56] Philippine Electricity Market Corporation (n.d.), Market Development - Retail. Philippines. https://www.wesm.ph/market-development/retail (accessed 1 August 2024).

[57] Department of Energy Philippines (2020), 2019 Power Situation Report. Philippines. https://doe.gov.ph/sites/default/files/pdf/electric_power/2019-power-situation-report.pdf (accessed 1 August 2024).

Trading Market:

- Through the WESM (Wholesale Electricity Spot Market) which was established in 2006 with the support of ADB and JICA (from the Luzon grid, followed by operations in the Visayas grid in 2010 and Mindanao grid started operations by June 2022).
- Luzon accounts for 80% of the transaction volume, and Meralco is the largest buyer.

Retail:

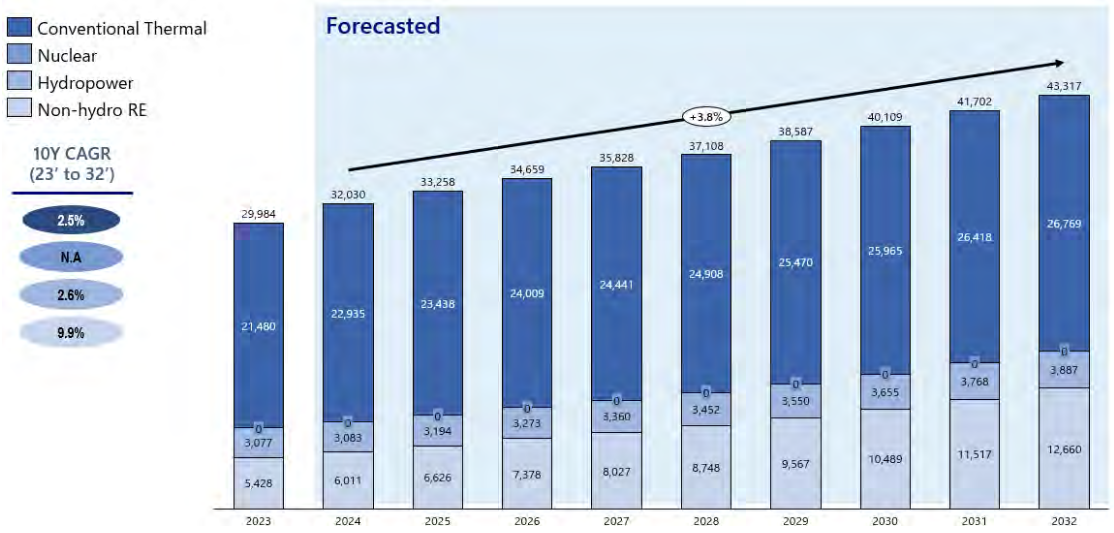
- Liberalised for contracted power of >500kW. There are retail electricity suppliers (RES) and PDU subsidiaries (for retail operations within PDU jurisdiction, called local RES). DSOs oversee retailing in non-liberalised area.
- Meralco accounts for nearly half of electricity sales in 2020. Meralco is the largest privately-owned electric utility with a market capitalisation of approximately USD6.6bn in end-2021. It contributed 43,572 GWh or 101,756 GWh total energy sales in Philippines and serves about 7.5mn customers.

100% FDI was allowed for power generation in the Philippines since 2022 by Department of Energy. On 29th September 2022, the Department of Justice (DOJ) issued an opinion that foreign investors in RE projects should be able to hold 100% ownership and approved. On 20 October 2020, the DOE adopted a circular on the guidelines for the third Open and Competitive Selection Process (OCSP3) in the awarding of renewable energy service contracts, allowing for 100% foreign ownership in large-scale geothermal exploration, development, and utilisation projects[58].

Philippines' energy capacity is projected to increase at a CAGR of 3.8% to 43,317 MW by 2032, with 29% of energy projected to be from non-hydro renewables.

[58] ASEAN Briefing (2023), Philippines Opens Renewable Energy to Full Foreign Ownership. https://www.aseanbriefing.com/news/philippines-opens-renewable-energy-to-full-foreign-ownership/ (accessed 2 August 2024).

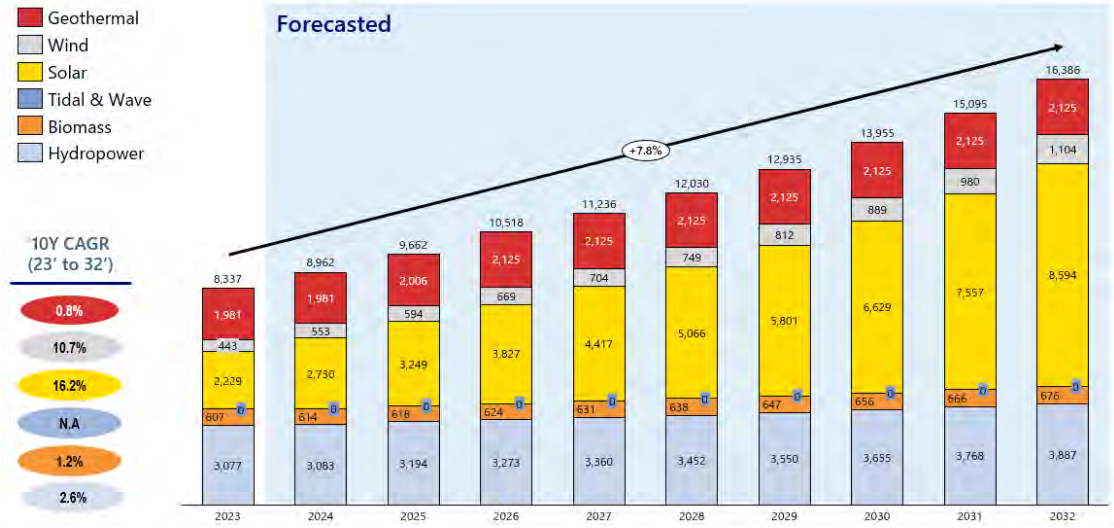
Figure A.11 Total Energy Mix Capacity MW (2023–2032F)



Source: Created by authors based on Fitch Solutions.

Solar PV is expected to dominate the Philippines renewable energy sector, which potential almost account for 8,594MW.

Figure A.12 RE Energy Mix Capacity MW (2023–2032F)



Source: Created by authors based on Fitch Solutions.

(2) Bilateral Trading

In the Philippines, The Net-Metering is the first non-fiscal incentive mechanism fully implemented under the Renewable Energy (RE) Act of 2008. The Net-Metering is the first non-fiscal incentive mechanism fully implemented under the Renewable Energy (RE) Act of 2008. Through the installation of solar photovoltaic (PV) panels up to 100 kW, house owners and commercial establishments can now partly satisfy their electricity demand

by themselves. Excess power generated from the solar PV installation will be delivered to the local distribution grid. This will be used to offset the end-user's electricity consumption. In other words, end-users become 'prosumers' or producers and consumers of electricity at the same time. In effect, end-users are able to generate savings on their electricity bill and protect themselves against rising electricity prices.

Figure A.13 Process of Realisation of Net Metering

Source: Department of Energy Philippines, 2021[59]

Other than the net-metering scheme, Customers can select their energy suppliers through RCOA and GEOP. While direct agreements between end-users and GenCos are possible, they are usually conducted through RES.

Retail Competition and Open Access (RCOA)[60]

- Eligibility: Past 12-month average historical monthly peak demand of ≥ 500 kW are considered contestable customers.
- Pricing is not regulated by the ERC.

Green Energy Option Program (GEOP)[61]

- Eligibility: Customers with 12-month average historical monthly peak demand of ≥ 100 kW.
- Limited only to electricity suppliers that provide renewable energy, as certified by ERC.

[59] Department of Energy Philippines (2021), Guidebook on Net Metering in the Philippines. Philippines. https://doe.gov.ph/sites/default/files/pdf/announcements/draft-guidebook-on-net-metering-2021.pdf (accessed 2 August 2024).

[60] Department of Energy Philippines (2015), Retail Competition and Open Access (RCOA). Philippines. https://doe.gov.ph/philippine-grid-net-generation?q=rcoa (accessed 2 August 2024).

[61] Department of Energy Philippines (2022), Green Energy Option Program (GEOP). Philippines. https://doe.gov.ph/sites/default/files/pdf/consumer_connect/Primer%20on%20Green%20Energy%20Option%20Program.pdf (accessed 2 August 2024).

The Green Energy Option Program (GEOP) is an initiative under the Renewable Energy Act of 2008 to empower electricity end-users to choose purely from Renewable Energy Resources for their electricity requirements. Eligible end-users for this programme are entities with an average peak demand of 100 kW for the past 12 months. IEMOP, as the Central Registration Body, is set to commence the Green Energy Option Program (GEOP) starting on 3 December 2021.

The Direct Power Purchase Agreement (DPPA) is a key component of the GEOP. Under the DPPA, eligible consumers, such as large commercial and industrial customers, can directly negotiate and enter into power purchase agreements with renewable energy generators This arrangement allows consumers to meet their sustainability goals and support the development of renewable energy projects.

However, the GEOP is currently not a regulated activity. GEOP is voluntary policy mechanism under the Renewable Energy Act of 2008 that allows electricity end-users to choose Renewable Energy as their source of energy. It is a non-regulated activity that provides the option to end-users to contribute to the development and utilisation of RE in a least cost and sustainable manner.

(3) Electricity Market Condition

In the Philippines, there are wholesale market, capacity market, and voluntary carbon credit market, but as of the period of this research project, there is no demand response programme.

①Wholesale market

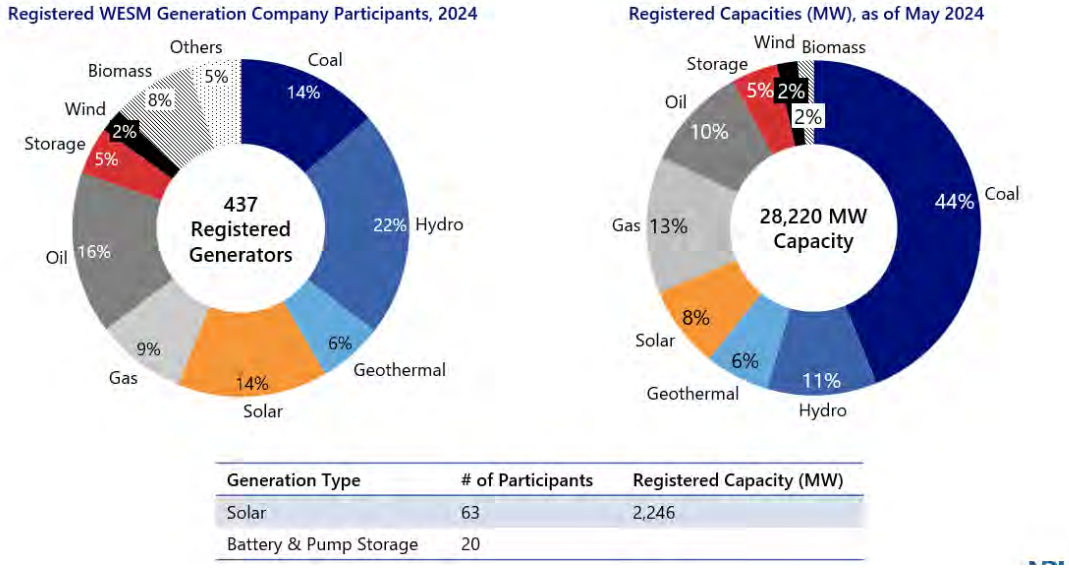
The Philippine Wholesale Electricity Spot Market (WESM) is a centralised venue for buyers and sellers to trade electricity as a commodity. The Philippine Electricity Market Corporation (PEMC) was incorporated in November 2003 as a non-stock, non-profit corporation upon the initiative of the Department of Energy (DOE) with representatives from the various sectors of the electric power industry.

The PEMC served as the autonomous group market operator and governing body of the Philippine Wholesale Electricity Spot Market (WESM) for over ten years.

The WESM is a centralised venue for buyers and sellers to trade electricity as a commodity where prices are determined based on actual use (demand) and availability (supply).

Around 28.2 GW Capacity has been registered in the WESM. It is mostly occupied coal and hydro but solar is also registered as equivalent to 2.2GW.

Figure A.14 Transaction Record in Wholesale Market

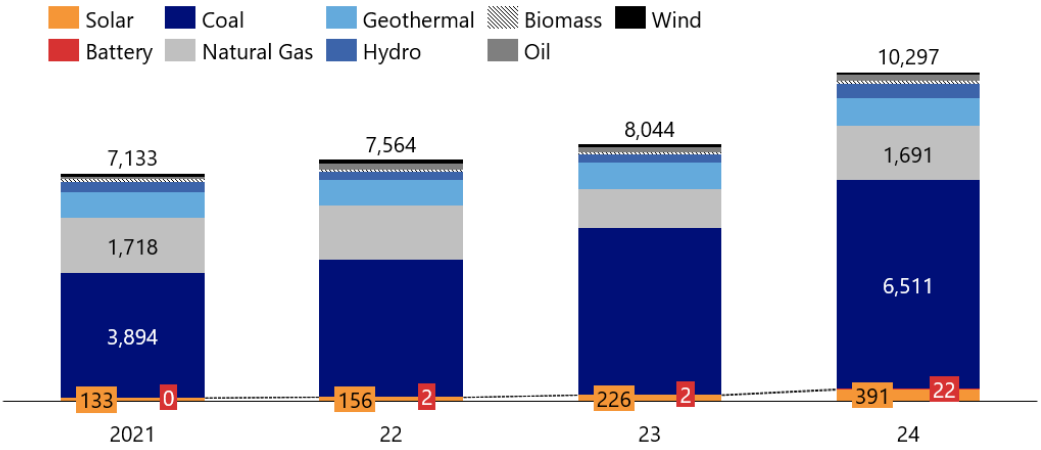


Generation Type	# of Participants	Registered Capacity (MW)
Solar	63	2,246
Battery & Pump Storage	20	

Source: Created by authors based on Philippine Electricity Market Corporation[62]

As a recent trend of Wholesale market, the amount of Solar and BESS has been gradually increased since 2021.

Figure A.15 Transaction Record (WESM Generation Mix (GWh), 2021–2024)



Source: Created by authors based on Philippine Electricity Market Corporation[63]

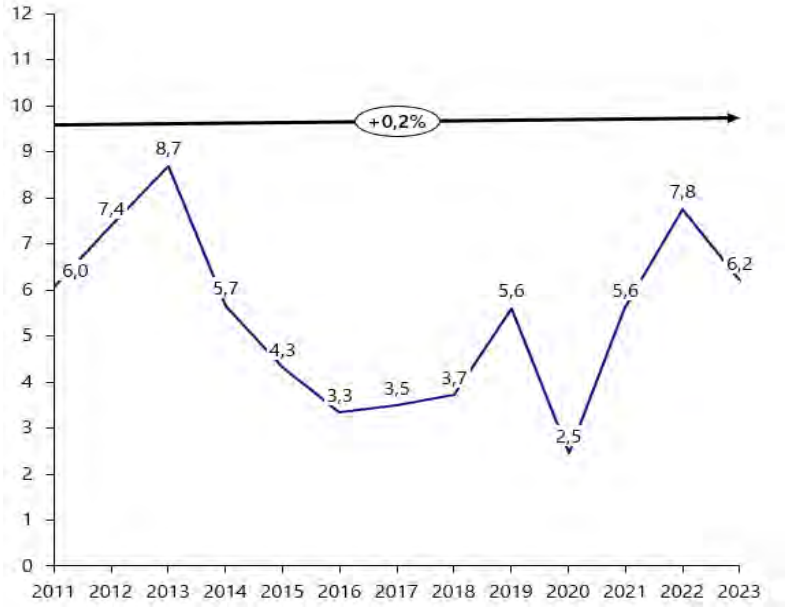
The annual average of transaction prices over the last 13 years has ranged between 3.3 and 8.7 Php/kWh, with an average annual growth rate of 0.2% and a slight upward trend, which is expected to be around 6–8 Php/kWh in the future. In the future, the WESM price

[62] Philippine Electricity Market Corporation (2024), Annual Market Assessment Report. Philippines. https://www.wesm.ph/downloads/download/TWFya2V0IFJlcG9ydHM=/MzIyNg== (accessed 1 August 2024).

[63] Philippine Electricity Market Corporation (2024), Annual Market Assessment Report. Philippines. https://www.wesm.ph/downloads/download/TWFya2V0IFJlcG9ydHM=/MzIyNg== (accessed 1 August 2024).

is forecasted to be around 6–8 Php/kWh based on the interview with IEMOP. The future construction of a nuclear power plant could have a huge impact on the WESM market.

Figure A.16 WESM price Trend (Php/kWh)



Source: Created by authors based on Philippine Electricity Market Corporation[64]

②Ancillary market

Different types of ancillary services have different participation requirements and participation capacities, and RR has the highest service rate at 2.25 Php/kWh.

[64] Philippine Electricity Market Corporation (2024), Annual Market Assessment Report. Philippines. https://www.wesm.ph/downloads/download/TWFya2V0IFJlcG9ydHM=/MzIyNg== (accessed 1 August 2024).

Figure A.17 Ancillary Service Overview

AS Type		Requirement	Currently used technology *Based on current ASP contract list*	Firm AS Capacity (MW)						Ancillary Service Rate (Php /kW/Hr)
				Luzon		Visayas		Mindanao		
				Peak	Off peak	Peak	Off peak	Peak	Off peak	
RR	Regulating Reserve	4% of the hourly system demand	• BESS • Diesel • Gas Fired • Hydro	160-200	90-150	60-80	46-60	40-70	40	2.25
CR	Contingency Reserve	the most heavily loaded generating unit online and its scheduled reserve	• BESS • Coal • Diesel • Hydro	500-580	340-420	30-60	30-90	120-150	100-140	1.50
DR	Dispatchable Reserve	the second most heavily loaded generating unit on-line and its scheduled reserve	• Coal • Diesel • Hydro	400-480	400-460	40-80	40-80	90-140	90-140	0.85
RPS	Reactive Power Support	Dependent on system voltage condition	• Coal • Diesel • Hydro	-	-	-	-	-	-	NA
BSS	Black Start Service	one black start plant per restoration highway	• Diesel • Gas Fired • Geothermal • Hydroe	-	-	-	-	-	-	NA

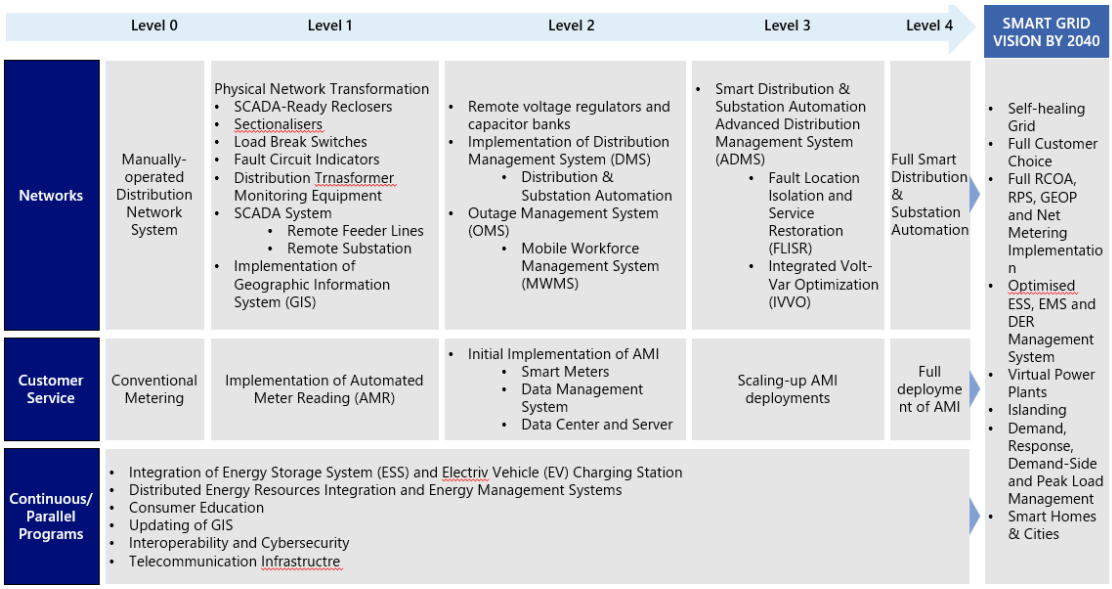
Source: Created by authors based on Philippine Electricity Market Corporation[65]

(4)Future Opportunities for DES

A DoE circular said the policy formulation committee will propose the national strategy for the smart grid, including Demand Response until 2040 with major emphasis on the possible impact on the price of electricity.

[65] Philippine Electricity Market Corporation (2024), Annual Market Assessment Report. Philippines. https://www.wesm.ph/downloads/download/TWFya2V0IFJlcG9ydHM=/MzIyNg== (accessed 1 August 2024).

Figure A.18 Smart Distribution Utility Roadmap (SDUR)



Source: Created by authors based on Department of Energy Philippines[66]

In Department Circular No. 002020-02-0003 stated the promotion of Cyber security for Distributed Energy System with facilitating the installation of VPP and Demand Response.

In Department Circular No. 002020-02-0003, providing a national smart grid policy framework for the Philippines electric power industry and roadmap for distribution utilities, clearly stated the following points, which facilitate the VPP and DR as well as installation of DERs[67]:

- 4.4. Optimized Energy Storage Systems (ESSs), Energy Management Systems (EMSs), and Distributed Energy Resources (DERs) Management Systems;
- 4.5. Virtual Power Plant Integration;
- 4.7. Demand Response, Demand-Side and Peak Load Management
- Also, this circular mentioned the importance of promoting the cyber security
- 5.7.1. To prevent potential cyber-attacks/breach during SG deployments, GenCos, TNP, and DUs shall develop a cybersecurity infrastructure and ensure cost-effective protection.

[66] Department of Energy Philippines (2019), Annex 1: Smart Distribution Utility Roadmap (SDUR). Philippines. https://doe.gov.ph/sites/default/files/pdf/announcements/draft_dc_12_july_2019_annex_a_sdu_roadmap_for%20_dus.pptx (accessed 2 August 2024).

[67] Department of Energy Philippines (2020), Department Circular No. DC2020-02-0003. Philippines. http://doe.gov.ph/sites/default/files/pdf/issuances/dc2020-02-0003.pdf (accessed 2 August 2024).

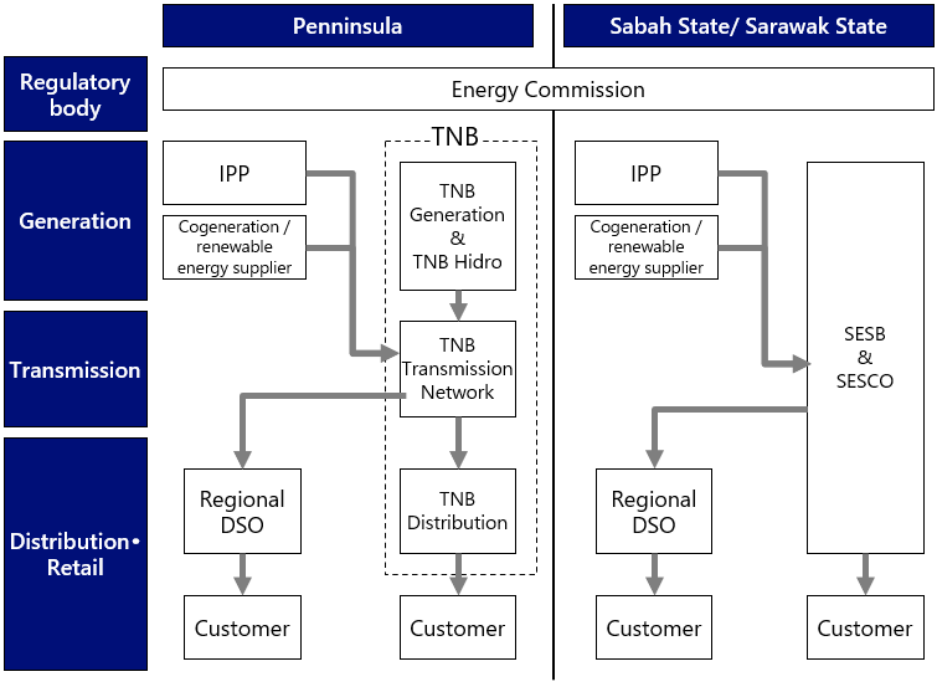
- 5.7.2. Cybersecurity infrastructure to be developed shall be compliant with all relevant laws and regulations as well as internationally accepted standards at the appropriate level of adoption and application.

1-1-3. Malaysia

(1) Market Structure

Malaysia's energy market allows for private participation in generation segment, but the transmission/distribution/retail is fully controlled by state owned operators.

Figure A.19 Overview of the Electricity System in Malaysia



Source: Created by authors based on Science Direct[68]

In Malaysia, there are differing states of deregulation depending on the location.

[68] ScienceDirect (2021), Malaysia's electricity market structure in transition. https://www.sciencedirect.com/science/article/abs/pii/S0957178721001004 (accessed 5 August 2024).

Table A.3 Status of Deregulation in Malaysia

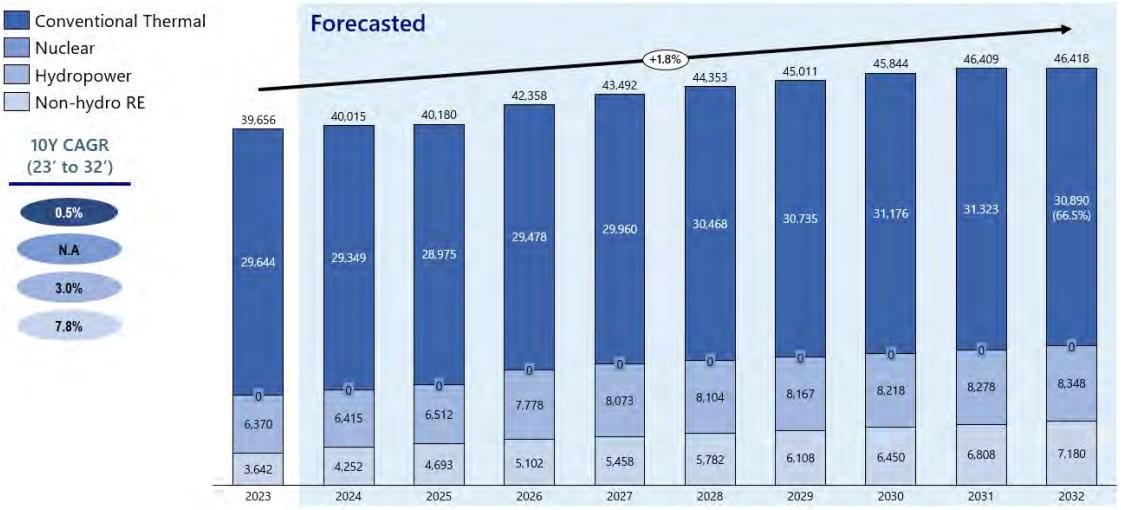
Separation of Generation and Transmission	Retail Liberalisation	Trading market
Both Peninsula and East Malaysia are vertically integrated. For transmission, TNB occupies peninsula, SESB occupies Sabah, and SESCO occupies Sarawak	In principle, it is an exclusive market where TSO does distribution and retail. However, dozens of companies are licensed for distribution and retail in limited areas such as industrial parks and resorts.	There is no wholesale trading/market in Malaysia. There is no ancillary service market in Malaysia.

Source: Created by authors based on International Journal of Electronics and Electrical Engineering[69]

FDI is generally restricted to a maximum 49% for power sector in Malaysia with certain exceptions (typically on a case-by-case basis)[70]. For example, in 2015, the government made an exception for the acquisition of IMDB's power assets by China General Nuclear for 9.83 billion ringgit. It was the largest, and so far, only instance in which the Malaysian government has made an exception to the foreign equity rule and allowed a non-Malaysian entity to acquire 100 per cent of the equity in an IPP.

Malaysia energy capacity is estimated to achieve CAGR of 1.8% to reach 46,418MW by 2032, with conventional thermal estimated to account for 66%.

Figure A.20 Total Energy Mix Capacity MW (2023-2032F)



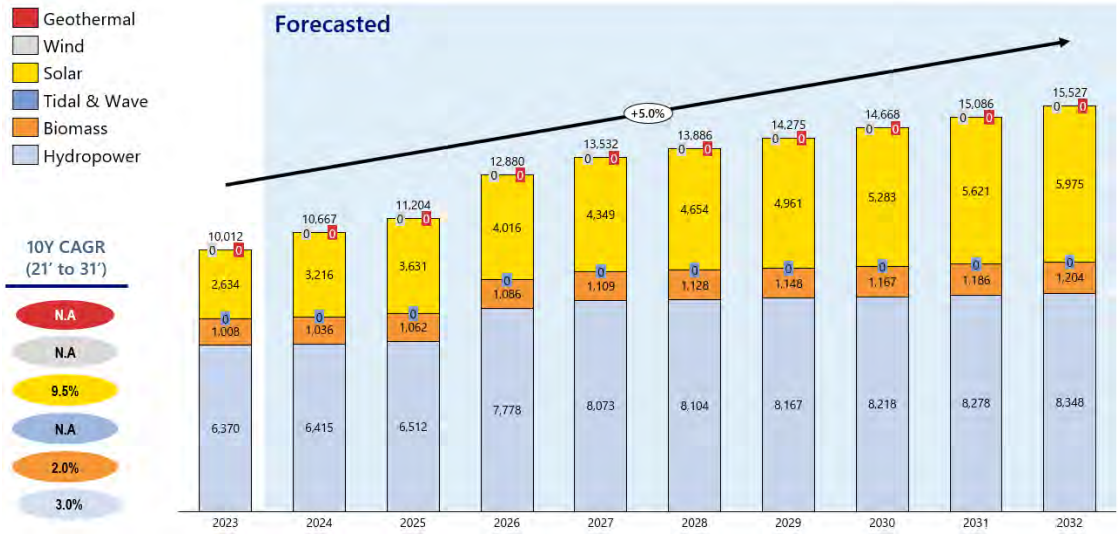
Source: Created by authors based on Fitch Solutions.

[69] International Journal of Electronics and Electrical Engineering (2020), De-Regulation of Electricity Industry: A Malaysian Perspective. https://www.ijeee.net/uploadfile/2020/0619/20200619112247349.pdf (accessed 5 August 2024).

[70] Asia Business Law Journal (2021), Renewable energy regulations in Malaysia. https://law.asia/renewable-energy-regulations-malaysia/ (accessed 5 August 2024).

For renewable energy, hydropower is expected to dominate Malaysia's renewable sector, followed by solar power growth, which is estimated to amount to 5,975 MW by 2032.

Figure A.21 RE Energy Mix Capacity MW (2023-2032F)



Source: Created by authors based on Fitch Solutions.

(2) Bilateral Trading

In Malaysia, the Net-Metering scheme (NEMS) allows energy users to generate energy locally using Solar and sell back excess generation to the grid. The NEMS have gone through a few renditions over the years:

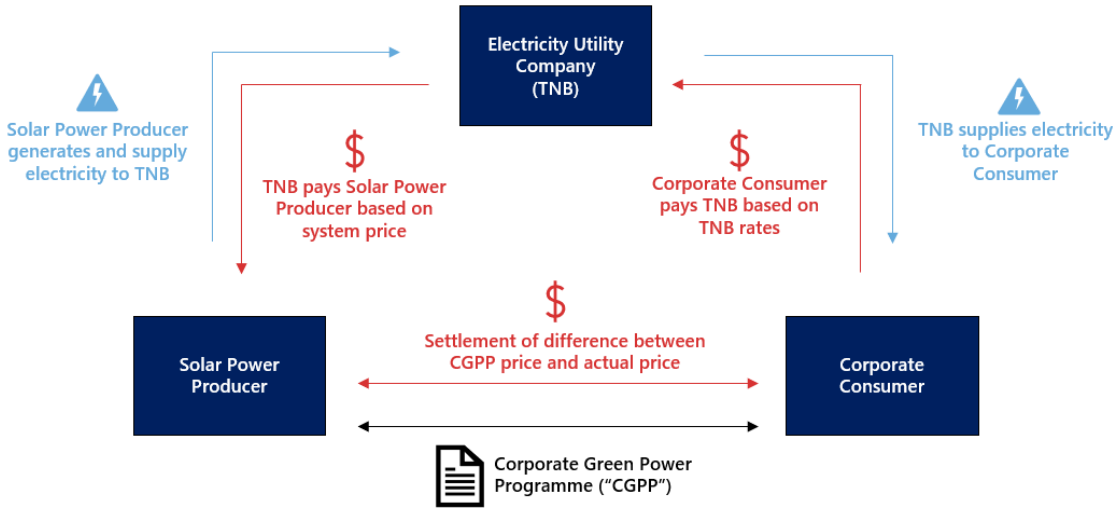
- In November 2016, NEMS 1.0 started with a 500 MW quota until 2020 to encourage Renewable Energy (RE) adoption. The concept was simple, solar PV systems would first power your own place, and any extra energy would be sold to the grid at market rates.
- In January 2019, NEMS 2.0 was introduced as the true net energy metering, letting participants export excess solar power back to the grid on a 'one-on-one' basis[71].
- In December 2020, NEMS 3.0 was introduced and any extra electricity generated will be sent back to the grid and credited to the users account on a 1:1 offset basis for future bills. NEMS 3.0 will be divided into the following three initiatives/categories: (1) NEM Rakyat Programme (Residential), (2) NEM GoMEn Programme (Government Buildings) and (3) NOVA Programme (Commercial, Industrial, Agriculture and Mining Buildings). The quotas allocated were 100 MW,

[71] Sustainable Energy Development Authority Malaysia (n.d.), Net Energy Metering (NEM) 2.0. Malaysia. https://www.seda.gov.my/reportal/nem2/ (accessed 6 August 2024).

100MW and 300MW respectively and are closed for application as of 31st December 2023[72].

Other than the net-metering scheme, The Corporate Green Power Programme ('CGPP') was launched in 2022 to allow corporate consumers to purchase power from solar power producers via direct delivery. The CGPP gives corporations the option to procure green electricity via a VPP, with a total quota of 600MW. Additional quota of 200MW was announced on Mar 23, 2023[73].

Figure A.22 CGPP Scheme



Source: Created by authors based on Lexology[74]

Under the CGPP, companies can sign VPPAs and sell electricity to grid, but the total export capacity is limited to between 5 MW and 30 MW. The applications for the CGPP programme will be open util 31 Dec 2023 or until the quota is fully subscribed. Under the CGPP programme, eligible companies could enter into a Corporate Green Energy Agreement (PTHK) with solar energy generators for the sale and purchase of Renewable Energy (RBE) virtually through mutually agreed terms and conditions. The Scheme will be opened until 31 December 2025 or until the allocation is fully utilised (whichever is earlier). In terms of criteria, the SPP must develop and operate a new solar power plant with export capacity between 5MW to 30MW and complete development by 2025. The SPP shall either be a local company with a minimum 51% Malaysian equity interest or a consortium with a minimum 51% Malaysian equity interest and consisting of at least one local company.

[72] Sustainable Energy Development Authority Malaysia (n.d.), Net Energy Metering (NEM) 3.0. Malaysia. https://www.seda.gov.my/reportal/nem/ (accessed 6 August 2024).

[73] Suruhanjaya Tenaga Energy Commission (2023), Information Guide For Corporate Green Power Programme. Malaysia. https://www.st.gov.my/en/contents/files/download/154/Guide_CGPP-_31_Jan_2023.pdf (accessed 7 August 2024).

[74] Lexology (2022), Malaysia's Corporate Green Power Programme: Virtual Power Purchase To The Fore. https://www.lexology.com/library/detail.aspx?g=c65dbbc5-51ea-4af5-be55-91bd722c5bdc (accessed 6 August 2024).

(3) Electricity Market Condition

In Malaysia, there are no wholesale market and capacity market but there is voluntary carbon credit market although it is still in early stage as the first and only carbon credit auction was conducted in 2023. There is no DR programme as it follows a single-buyer model, power generated is purchased by the state-owned power entity TNB and then sold directly to consumers.

①Carbon Credit Market

Malaysia has the Bursa Carbon Exchange (BCX) which is the first Shariah-compliant carbon exchange in the world. The BCX is a global spot exchange that enables corporates to take practical climate mitigation action through the trading of carbon credits. BCX conducted Malaysia's inaugural carbon credit auction in March 2023.

Table A.4 BCX Auction Details

Objective	The auction was meant to facilitate the price-discovery of carbon credits from two new products offered by the BCX - the Global Technology-Based Carbon Contract (GTC) and the Global Nature-Based Plus Carbon Contract (GNC+)
Outcomes	There was strong interest and healthy price signal by the domestic corporate sector, notably government-linked companies and financial institutions which will help facilitate the development of future carbon credit projects.

Global Technology-Based Carbon (GTC) Contract	**Global Nature-Based Plus Carbon (GNC+) Contract**

• The GTC Contracts were oversubscribed and cleared at RM18.50 per contract.
  ○ The carbon credits were supplied by Vitol Asia.
• The GTC Contracts featured carbon credits from the Linshu Biogas Recovery and Power Generation Project in China. The project had benefits that align with the United Nations Sustainable Development Goals (UN SDG).
	• The GNC+ Contract fetched a clearing price of RM68.00 per contract.
	  ○ The carbon credits were supplied by Vitol Asia.
	• The GNC+ Contracts featured carbon credits from the Southern Cardamom Project, which is a REDD+ (Reducing Emissions from Deforestation and Forest Degradation) project from Cambodia that comes with climate, community and biodiversity (CCB) standard that provides additional co-benefits, contributing to the livelihoods of local communities and biodiversity conservation.

Source: Created by authors based on Bursa Carbon Exchange[75]

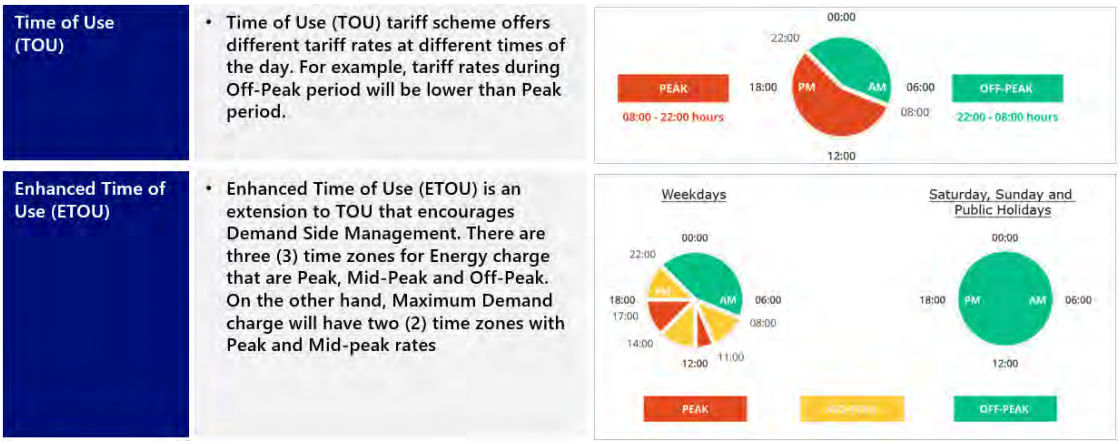
The auction, which was carried out electronically, saw participation with 15 buyers from various industries purchasing a total of 150,000 Verra-registered carbon credits.

②Time of Use (TOU) and Enhanced Time of Use (ETOU)

There are no DR Programmes in Malaysia. Instead, the Time of Use (TOU) and Enhanced Time of Use (ETOU) mechanism is used to encourage customers to lower their electricity consumption during peak hours.

[75] Bursa Carbon Exchange (2023), BURSA CARBON EXCHANGE SUCCESSFULLY COMPLETES MALAYSIA'S INAUGURAL CARBON AUCTION. Malaysia. https://bcx.bursamalaysia.com/index.php?rp=bcx_pressrelease_17march2023 (accessed 7 August 2024).

Figure A.23 TOU and ETOU Mechanism



Source: Created by authors based on Tenaga Nasional Berhad[76]

(4) Future Opportunities for DES

There are limited opportunities for DES in Malaysia as the mechanisms to conduct such a business are not well established.

1-1-4. Thailand

(1)Market Structure

Thailand's energy market only allows private players for generation as transmission/distribution and retail is limited to state owned operators.

Overview of the Electricity System in Thailand[77,78,79]

Regulatory Body:

- The Ministry of Energy (MOEN) oversees the Electricity Generating Authority of Thailand (EGAT), Metropolitan Electricity Authority (MEA), Provincial Electricity Authority (PEA).

[76] Tenaga Nasional Berhad (n.d.), Frequently Asked Questions. Malaysia. https://www.mytnb.com.my/faq (accessed 7 August 2024).

[77] Thailand Board of Investment (2023), Thailand's Electricity Market. Thailand. https://www.boi.go.th/index.php?page=electricity (accessed 7 August 2024).

[78] Electricity Generating Authority of Thailand (n.d.), EGAT Profile. Thailand. https://www.egat.co.th/home/en/about-egat/ (accessed 8 August 2024).

[79] Thailand Development Research Institute (2023), Electricity liberalisation, the way of leading the country towards clean, affordable, and equitable electricity. Thailand. https://tdri.or.th/en/2023/11/electricity-liberalisation-the-way-of-leading-the-country-towards-clean-affordable-and-equitable-electricity/ (accessed 8 August 2024).

- The National Energy Policy Office (NEPO) is responsible for power generation planning, investment promotion, transmission and distribution planning, investment promotion, wholesale price regulation, etc.

Generation:

- Private participation in the generation business is allowed in Thailand. Generation companies include EGAT, IPPs, SPP, VSPP and Foreign imports

Transmission / Distribution:

- Transmission is exclusively owned and operated by EGAT. Electricity generated by IPP and SPP operators is wholesaled to EGAT and transmitted using EGAT's transmission facilities. Currently there are no private participation allowed in transmission.

Backbone system of 500, 230, 115, 69kV.

- Distribution is exclusively owned and operated by MEA and PEA. MEA distributes to the metropolitan area and PEA distributes to rural areas. Currently there are no private participation allowed in distribution.
- MEA: High voltage: 24, 12kV, low voltage: 380, 220V.
- PEA：High voltage: 33, 22, 19kV, low voltage: 400, 230V.

Trading Market:

- EGAT occupies transmission, MEA and PEA occupies retail and there is no wholesale or ancillary market trading.

Retail:

- Exclusively operated by MEA and PEA.

In the past, liberalisation of retail supply was considered along with privatisation of EGAT (which was withdrawn) due to the 2000–2001 California power crisis. In March 2006, the Supreme Administrative Court ruled against privatisation, citing conflicts of interest, public hearing irregularities and the continued right of expropriating public land. Hence, EGAT will purchase electricity from IPPs/SPPs etc. as an off-taker and to power distribution companies and large customers.

100% FDI allowed for power generation in Thailand, but foreign company need to apply for investment promotion certificate to own land for project It is important to note that a non-Thai company cannot own land under the Land Code[80]. Therefore, a majority foreign-owned company must apply for an investment promotion certificate from the Board of

[80] Thailand Board of Investment (2023), Investment Promotion Guide. Thailand. https://www.boi.go.th/upload/content/BOI_A_Guide_EN.pdf (accessed 8 August 2024).

Investment (BOI) for the right to own land used in the project.

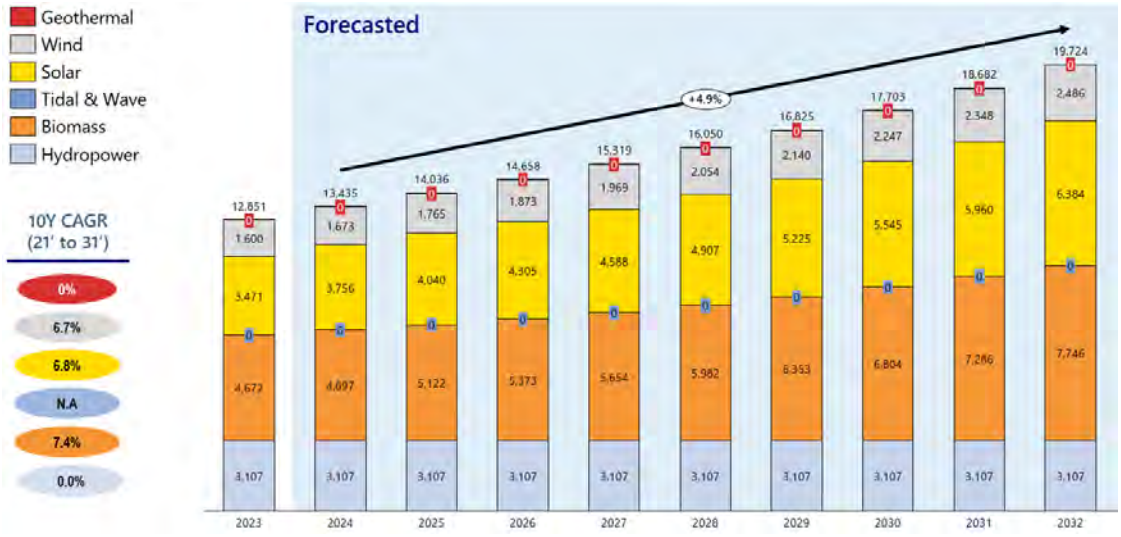
Thailand energy capacity is projected to increase at a CAGR of 2.8% to 71,043 MW by 2032, with 72% of energy projected to come from conventional thermal.

Figure A.24 Total Energy Mix Capacity MW (2023–2032F)

Source: Created by authors based on Fitch Solutions.

For renewable energy, biomass is expected to dominate the renewable energy sector, followed by Solar, which potential almost account for 6,384 MW.

Figure A.25 RE Energy Mix Capacity MW (2023–2032F)



Source: Created by authors based on Fitch Solutions.

(2) Bilateral Trading

In Thailand, the Net-Metering scheme allows household that have installed rooftop solar

panels to participate in selling excess electricity. However, the Thailand government announced in 2023, that they will put the net-metering on hold as results from a feasibility study conducted by the Energy Ministry surfaced many issues of the net metering scheme[81].

Other than the net-metering scheme, Thailand has issued in 2020, a new regulation setting out criteria and conditions for power purchase agreements (PPAs) for very small power producers (VSPPs) under the Community Power Plants for the Local Economy project. To qualify as a VSPP, a power producer must generate no more than 10 MW per project and must comply with the requirements and restrictions set by the Executive Committee of Power Purchase from Community Power Plant Projects[82].

Furthermore, prospective VSPPs may only use one of the following:

- Biomass
- Biogas from wastewater or waste
- Biogas from biofuel
- A hybrid of biomass with biogas (wastewater or waste)
- A hybrid of biogas (biofuel) with solar power

(3) Electricity Market Condition

In Thailand, there are no wholesale market and capacity market but there is voluntary carbon credit market. There is no DR programme as Thailand is still actively testing it through pilot projects as of the time in writing this report.

①Carbon Credit Market

Thailand has the voluntary carbon credit programme called Thailand Voluntary Emission Reduction Programme (T-VER), which supports the voluntary reduction of greenhouse gas emissions. It is established in 2014 and the development and registration of projects under this programme is overseen by Thailand Greenhouse Gas Management Organisation (TGO)[83]. Transaction method can either be over the counter or through

[81] Nation Thailand (2023), Household 'net energy metering' plan put on hold. Thailand. https://www.nationthailand.com/thailand/general/40029286 (accessed 13 August 2024).

[82] Tilleke & Gibbins (2020), Thailand Issues Regulations for Procurement of Electricity from Very Small Power Plants. https://www.tilleke.com/insights/thailand-issues-regulations-procurement-electricity-very-small-power-plants/3/ (accessed 13 August 2024).

[83] Thailand Greenhouse Gas Management Organisation (n.d.), Overview. Thailand. https://tver.tgo.or.th/index.php/en/en-about/en-overview (accessed 13 August 2024).

exchange platform with project type as follows[84]:

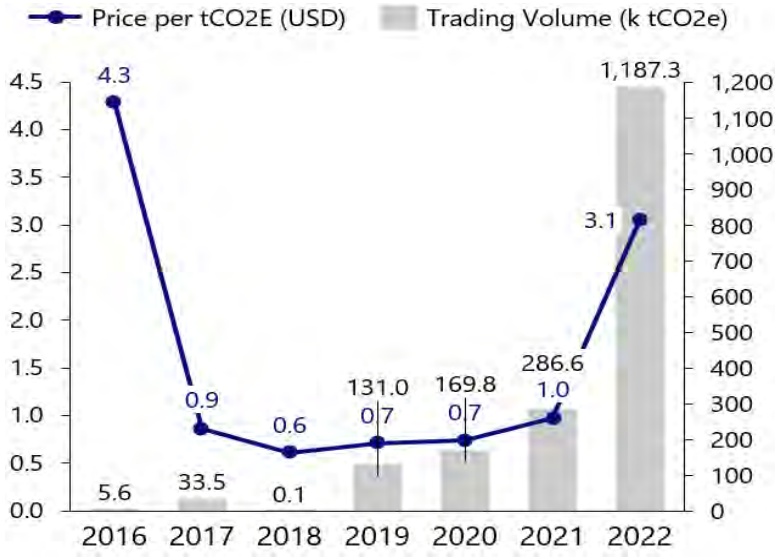
- Renewable energy or fossil fuel replacement
- Improvement of efficiency of electricity and heat generation
- Public transportation system
- Electric vehicle
- Improvement of efficiency of engine
- Improvement of efficiency of energy consumption in buildings and factories, and in households
- Natural refrigerant
- Clinker substitutes
- Solid waste management
- Domestic wastewater management
- Methane recovery and utilisation
- Industrial wastewater management
- Reduction, absorption, and removal of greenhouse gases from the forestry and agricultural sectors
- Capture, storage, and/or utilisation of greenhouse gases.

The carbon credit voluntary price in Thailand has traded at an average price of USD3.1 per tons in 2022, which is within the same price standard as that of international market[85].

[84] Thailand Greenhouse Gas Management Organisation (2023), Project Specifications - Project Type. Thailand. https://tver.tgo.or.th/index.php/en/en-standard/kar-phathna-khorngkar-en/khx-kahnd-khorngkar-en/std-en-project-type (accessed 13 August 2024).

[85] Kaohoon (2022), BCP shows 95% of its carbon credit trading in the Thai market in the first half of the year. https://www.kaohoon.com/news/548871 (accessed 13 August 2024).

Figure A.26 Carbon credit trading volume and price per tCO2e in T-VER (2017–2022)



Source: Created by authors based on Thailand Greenhouse Gas Management Organisation[86]

From 2016–2022, trading volume has been on an increase while prices have fluctuated based on demand.

②Demand Response Pilot Programmes

Thailand is still actively testing Demand Response through pilot projects and has recently conducted one for the year 2022 – 2023 to test the reduction of power consumption during system peak hours. It was conducted jointly by the Energy Policy and Planning Office (EPPO), the Energy Regulatory Commission (ERC), Metropolitan Electricity Authority (MEA) and Provincial Electricity Authority (PEA)[87]. Participants are expected to reduce electricity use from January to December 2023, aiming for a reduction of 50 MW during two peak periods: 13:30–16:30 and 19:30–22:30.

Additionally, the Electricity Generating Authority of Thailand (EGAT) has set up two new centres – (1) Renewable Energy Forecast Centre and (2) Demand Response Control Centre within EGAT to facilitate DR load aggregation[88]. It is currently in the pilot phase with a reduced load of 50MW and with the MEA and the PEA serving as the load aggregators. In

[86] Thailand Greenhouse Gas Management Organisation (n.d.), Voluntary carbon credit prices in Thailand. Thailand. https://carbonmarket.tgo.or.th/index.php?lang=TH&mod=Y2N0X3ByaWNl (accessed 13 August 2024).

[87] Metropolitan Electricity Authority (2023), MEA extends application deadline for Demand Response Pilot Project for 2022-2023 to reduce power consumption in Category 3, 4 and 5 according to EPPO policy from now until 31 Oct 2022. Thailand. https://www.mea.or.th/en/public-relations/corporate-news-activities/announcement/hnzp7wxgL (accessed 16 August 2024).

[88] Smart Energy International (2023), EGAT advances Thailand's smart grid development. https://www.smart-energy.com/industry-sectors/energy-grid-management/egat-advances-thailands-smart-grid-development/ (accessed 16 August 2024).

the future when the load aggregator role is open to private players, the new energy business will emerge with all aggregators operating under the Centre.

(4) Future Opportunities for DES

There are limited opportunities for DES in Thailand as the mechanisms to conduct such a business are not well established. However, the government have been actively testing DR pilot projects and this could lead to an increasing possibility for DES business in the near term.

1-1-5. Indonesia

(1)Market Structure

Indonesia's energy market only allows private players for generation as transmission/distribution and retail is limited to state owned operator Perusahaan Listrik Negara (PLN).

Overview of the Electricity System in Indonesia[89,90,91]

Regulatory Body:

- Kementarian Energi dan Sumber Daya Mineral (Ministry of Energy and Mineral Resources) determines Indonesia's energy policy and supervises and regulates electricity, gas, oil, mining and other business activities. Under the minister in charge, it is divided into: (1) oil and gas (2) electricity and energy utilisation (3) mining and geothermal. Under the Department of Electricity, there are the Department of Electricity Program Supervision and the Department of Business Administration.
- Role and Responsibility includes policy decision, policy enforcement, decision of standard, technical guidance / evaluation, etc.

Generation:

- Private participation is allowed.

[89] IEA (2022), Enhancing Indonesia's Power System. https://www.iea.org/reports/enhancing-indonesias-power-system (accessed 19 August 2024).

[90] Asian Development Bank (2021), How Different Electricity Pricing Systems Affect the Energy Trilemma: Assessing Indonesia's Electricity Market Transition. https://www.adb.org/publications/how-different-electricity-pricing-systems-affect-energy-trilemma-indonesia (accessed 19 August 2024).

[91] SEA information Platform for the Energy Transition (n.d.), Indonesia Power Sector Snapshot. https://www.sipet.org/power-sector-snapshot-indonesia.aspx (accessed 19 August 2024).

- High share of thermal power, low adoption of renewable energy and IPP fills the shortage of PLN supply. As of 2022, 60% of generation comes from PLN and subsidiaries and 40% from IPP.
- New energy projects can be procured under one of three tender processes – direct appointment, direct selection, and public auction. Under the tender methods, the key bid parameter is the price at which generators are willing to sell the electricity generated.

Transmission / Distribution:

- Fully owned and operated by state owned PLN and no foreign or private participation is allowed.
- In the competitive areas (Java, Bali, Sumatra), generation, transmission, and distribution are separated as business units, while in non-competitive areas, the vertical integration is maintained.

Trading Market:

- There is no wholesale market as all IPP power generation is taken off to PLN.
- Meanwhile, ancillary services like Frequency Control and Ancillary Services (FCAS), crucial for maintaining the stability of electricity supply and system capacity, are not adequately valued in the grid. Instead, the responsibility for grid stability and reliability rests with PLN, which manages its generation assets outside the market to provide these services.

Retail:

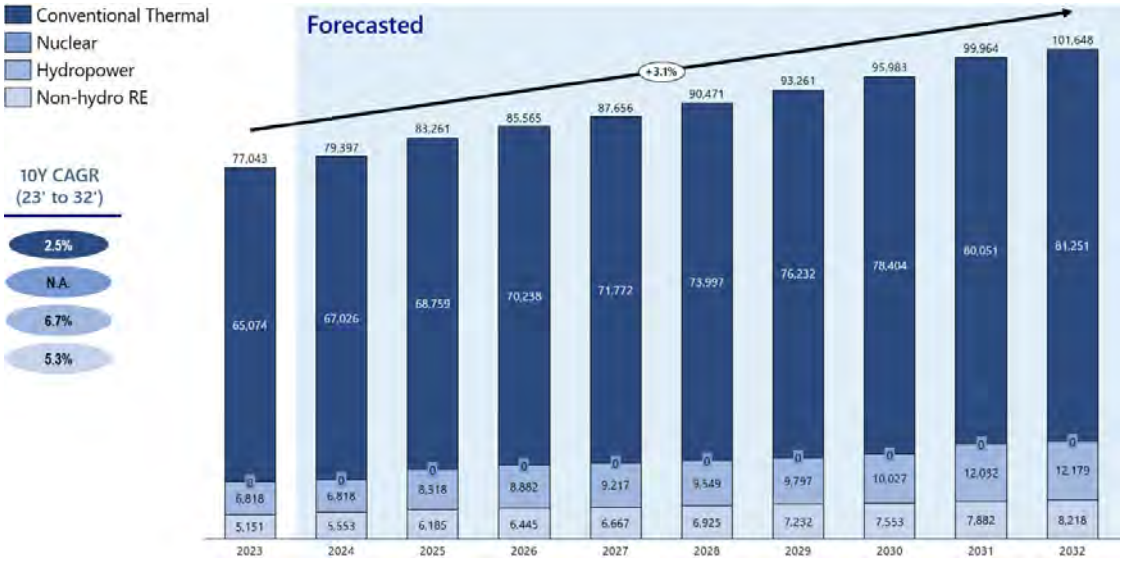
- PLN operates this entire segment. In the competitive area, each power distribution business unit conducts retail business. In non-competitive areas, nine regional branches and two regional subsidiaries operate as vertically integrated.

100% FDI is allowed for renewable energy in Indonesia since 2021, as it has entered a positive investment list that allows for 100% foreign ownership[92].

Indonesia energy capacity is projected to increase at a CAGR of 3.1% to 101,648 MW by 2032, with only 8% of energy to come from non-hydro renewables.

[92] ASEAN Briefing (2022), Indonesia's Positive Investment List: Sectors Open and Restricted to Foreign Businesses. https://www.aseanbriefing.com/news/indonesias-positive-investment-list-and-the-sectors-open-restricted-to-foreign-businesses/ (accessed 21 August 2024).

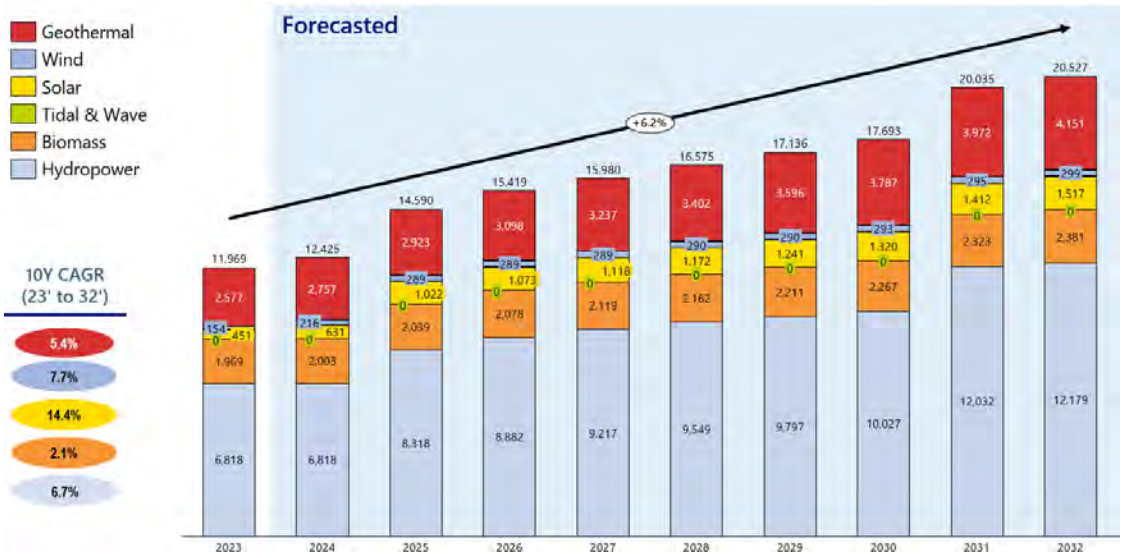
Figure A.27 Total Energy Mix Capacity MW (2023-2032F)



Source: Created by authors based on Fitch Solutions.

For renewable energy, hydropower is expected to continue dominate the Indonesian renewable energy sector, Solar is expected to see the highest growth rates.

Figure A.28 RE Energy Mix Capacity MW (2023–2032F)

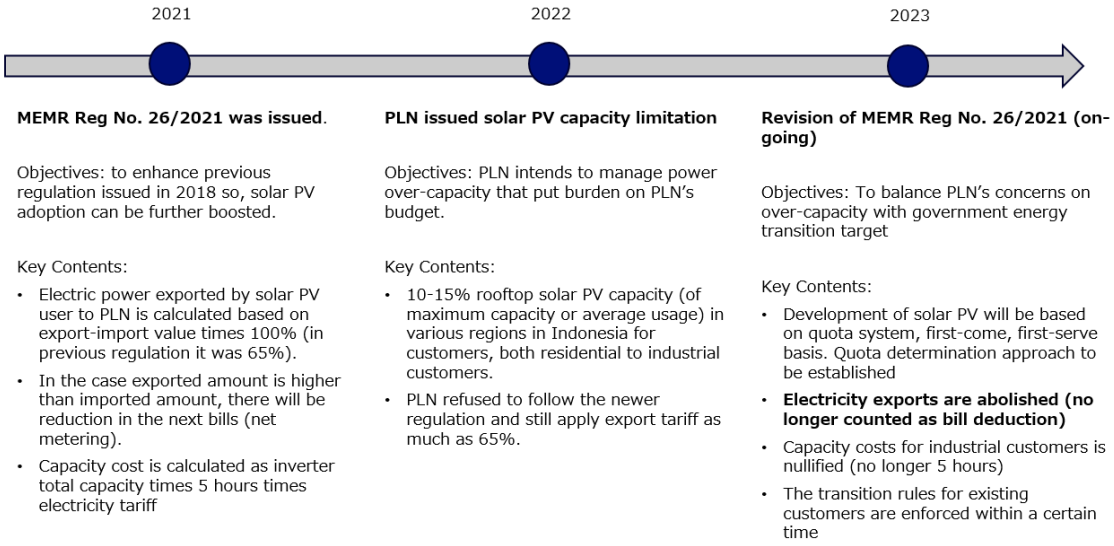


Source: Created by authors based on Fitch Solutions.

(2) Bilateral Trading

In Indonesia, the Net-Metering scheme allows household that have installed rooftop solar panels to participate in selling excess electricity back to the grid. However, the scheme is likely to be abolished in regions facing overcapacity.

Figure A.29 Timeline and details of net-metering abolishment



Source: Created by authors based on PV Magazine[93].

The PLN has limited rooftop PV capacity to 10%–15% in 2022 in various regions. This has triggered a review of existing regulations and the elimination of the net metering policy, which is expected to reduce demand for on-grid PV, especially in the residential sector, which has been increasing[94].

Other than the net-metering scheme, Indonesia allows for CPPA which PT Golden Blossom and SESM was the first hybrid CPPA scheme in renewable energy in Indonesia[95].

[93] PV Magazine (2024), Indonesian government abolishes net metering. https://www.pv-magazine.com/2024/02/28/indonesian-government-abolishes-net-metering/ (accessed 22 August 2024).

[94] ABNR Law (2024), Indonesia Issues New Rules on Operation of Rooftop Solar, Abolishes Net Metering. https://www.abnrlaw.com/news/indonesia-issues-new-rules-on-operation-of-rooftop-solar-abolishes-net-metering (accessed 22 August 2024).

[95] PV Magazine (2020), Indonesia's first PPA for large scale solar. https://www.pv-magazine.com/2020/03/04/indonesias-first-ppa-for-large-scale-solar/ (accessed 23 August 2024).

Table A.5 Electricity Price table of PLN

Category	Power Limit	Regular		Prepaid (IDR/kWh)
		Electricity Load Cost	Electricity Usage Cost (IDR/kWh) dan KVArh (IDR/KVArh)	
R-1/TR	900 VA – RTM	*)	1352	1352
	1300 VA	*)	1444.7	1444.7
	2200 VA	*)	1444.7	1444.7
R-2/TR	3500 -5500 VA	*)	1699.53	1699.53
R-3/TR	Above 6600 VA	*)	1699.53	1699.53
B-2/TR	6600 VA to 200 kVA	*)	1444.7	1444.7
B-3/TM	Above 200 kVA	**)	Peak-Time: K * 1035.78 Off-peak Time: 1035.78 KVArh = 1114.74 ****)	Not Available
I-3/TM	Above 200 kVA	**)	Peak-Time: K * 1035.78 Off-peak Time: 1035.78 KVArh = 1114.74 ****)	Not Available
I-4/TT	Above 30,000 kVA	***)	Peak and off-peak time: 996.74 KVArh: 996.74 ****)	Not Available
P-1/TR	6600 VA to 200 kVA	*)	1699.53	1699.53
P-2/TM	Above 200 kVA	**)	Peak-Time: K * 1035.78 Off-peak Time: 1035.78 KVArh = 1114.74 ****)	Not Available
P-3/TR		*)	1699.53	1699.53
L/TR,TM,TT		-	1644.52	Not Available

Notes:
*) Implementation of General Account 1:
General Account 1 = 40 (usage duration) * connected power (kVA) * Electricity Usage Cost
**) Implementation of General Account 2:
General Account 2 = 40 (usage duration) * connected power (kVA)* off-peak time usage cost
Usage duration: monthly kWh divided by connected power kVA
***) Implementation of General Account 3:
General Account 3 = 40 (usage duration) * connected power (kVA)* peak & off-peak time usage cost
Usage duration: monthly kWh divided by connected power kVA
****) Excess of Reactive power usage costs due to average power factor of each month being less than 0.85
K: A coefficient between 1.4 to 2.0 that will be determined by the PLN's Board of Directors in accordance with electricity load system.

Source: Created by authors based on PLN[96]

[96] PLN (2024), Penetapan-Tariff-Adjustment-Juli-September-2024. Indonesia. https://web.pln.co.id/statics/uploads/2024/07/Penetapan-Tariff-Adjustment-Juli-September-2024.jpg (accessed 23 August 2024).

Indonesia has limited application of CPPAs, but the country has growing interest to have a wider application of it as it can help large corporation to achieve their sustainable commitments.

There are several limitations on Indonesia's CPPA:

- The CPPA is only applicable for renewable energy, specifically Solar PV.
- There is a capacity threshold of Solar CPPA, which is larger than 500 kW (0.5 MW).
- The form of CPPA is the onsite PPA. Onsite PPA means that the corporate off-taker needs to be in the same area or vicinity of the power generator.
- Both power generators and corporate off-takers need to acquire licenses and approval from National Electricity Corporation (PLN).

(3) Electricity Market Condition

In Indonesia, there are no wholesale market and capacity market but there is voluntary carbon credit market formally introduced in 2023. There is no DR programme in Indonesia at the time of writing this report and there is only tariff system with different price between peak and off-peak to encourage customers to lower their electricity consumption during peak hours.

①Carbon Credit Market

To accelerate decarbonisation through voluntary market-based mechanisms, the Bursa Karbon Indonesia (IDXCarbon) carbon exchange market was formally launched in 2023[97]. Currently, trading is voluntary, but it will become mandatory once stricter pollution regulations are implemented. Emission limits are currently set only for the electric sector, so electric companies are expected to be the most active buyers in the market initially. However, as pollution limits are set for various sectors, other companies may join. SPE-GRK certificates allows trading internationally and between business sectors. The first carbon credit voluntary price was traded at $4.51 per tons, which is at a similar price standard with international pricing[98].

②Differentiating Electricity Tariff (Peak and Off-Peak Consumption Guidance)

The different tariffs between peak and off-peak hours are to encourage customers to

[97] Bursa Karbon Indonesia (IDX Carbon) (n.d.), About Us. Indonesia. https://idxcarbon.co.id/id (accessed 26 August 2024).

[98] Reuters (2023), Indonesia's president launches carbon emissions credit trading. https://www.reuters.com/sustainability/sustainable-finance-reporting/indonesias-president-launches-carbon-emissions-trading-2023-09-26/ (accessed 26 August 2024).

lower their electricity consumption during peak hours, which may lighten the grid load.

In Indonesia, PLN imposes specified tariffs at certain hours (peak and off-peak*) to ease the electricity consumption. However, the specified tariffs at peak and off-peak hours are only applicable to several group of customers, mostly large businesses or manufacturing (industrial) facilities. In terms of rates, the selected groups of customers will be given a coefficient multiplier ('K'), between 1.4 to 2[99]. The coefficient will multiply the electricity tariffs. Therefore, the electricity tariffs during peak hours can increase by 40 to 100%.

Applicable customers (customers that have specified tariffs during peak hours are):

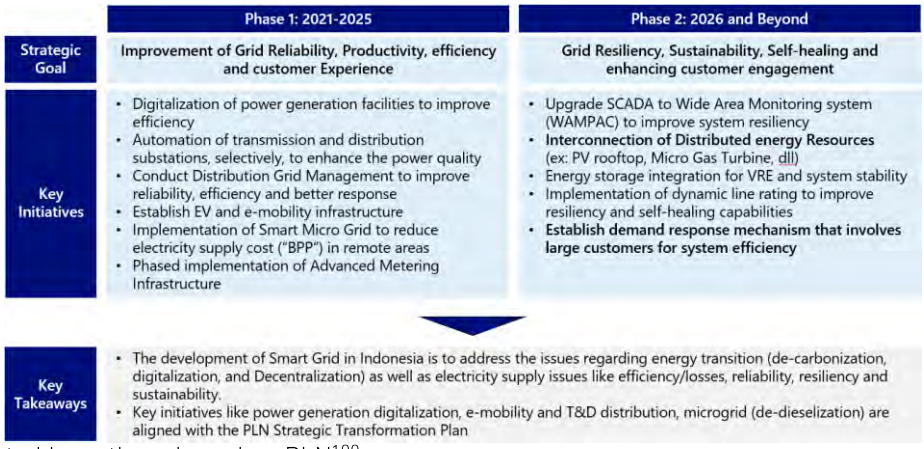
- B-3 Category and I-3 Category: Customer who have power limit beyond 200 kVA. Large offices to small-medium Industrial facilities.
- I-4 Category: Customer who has power limit beyond 30,000 kVA. This is mostly intended for large industrial facilities.
- P-1 category: small government office with power between 6.6 to 200 kVA.
- P-2 category: large government office with power beyond 200 kVA.

Note: Multiplier Coefficient ('K') is based on regional consumption and approved by PLN's board of directors.

(4) Future Opportunities for DES

The PLN has outlined its strategy on addressing energy transition through the Smart Grid Initiative.

Figure A.30 PLN Smart Grid Initiative



Source: Created by authors based on PLN[100]

[99] PLN (2024), Penetapan-Tariff-Adjustment-Juli-September-2024. Indonesia. https://web.pln.co.id/statics/uploads/2024/07/Penetapan-Tariff-Adjustment-Juli-September-2024.jpg (accessed 23 August 2024).

[100] PLN (2020), Pengembangan Smart Grid di Indonesia. Indonesia.

The aim for the smart grid initiative is to improve efficiency, reliability and resiliency through digitalisation, increase customer engagement (decentralisation) and increase VRE penetration through flexible grid (decarbonisation).

1-1-6. Viet Nam

(1)Market Structure

Viet Nam's power generation business is liberalised, with transmission/distribution and retail allowing for private players. However, Vietnam Electricity (EVN) still heavily controls the power market. The National Load Distribution Centre (NLDC) operates the wholesale market though it is yet to be fully operational in practice.

Overview of the Electricity System in Viet Nam[101,102,103]

Regulatory Body:

- Electricity Regulatory Authority (ERAV) established under Ministry of Industry and Trade (MOIT) in 2005, ERAV is the country's regulatory agency, responsible for establishing and supervising the power market, power planning, tariff regulation, and licensing. On the other hand, The MOIT is responsible for directing and supervising the development of the energy sector and reporting its findings to the prime minister.

Generation:

- As of 2020, EVN and its subsidiaries has majority of share (43%).
- EVN subsidiaries are divided into three companies (Power Generation Corporation No.1 to No.3) and there are two state-owned IPP operators – Petro Vietnam (PVN) and Vietnam National Coal and Mineral Industries Group (VINACOMIN).
- The rest are made up by few local IPPs and BOT.

Transmission / Distribution:

- As of March 2022, private investors can invest in the construction of the electrical transmission grid; and operate the electricity transmission grid in which they

---

https://iea.blob.core.windows.net/assets/8409fbba-7c53-4c95-89c2-3f653fd4ffd7/210226SmartGridsWS-PLNpresentation.pdf (accessed 27 August 2024).

[101] EVN - NLDC (2023), UPDATES ON VIETNAM POWER SYSTEM AND ELECTRICITY MARKET OPERATION. Vietnam. https://vepg.vn/wp-content/uploads/2023/06/EN_NLDC_Updates-on-Vietnam-Power-System-and-Electricity-Market.pdf (accessed 2 September 2024).

[102] SEA information Platform for the Energy Transition (n.d.), Vietnam Power Sector Snapshot. https://www.sipet.org/power-sector-snapshot-vietnam.aspx (accessed 2 September 2024).

[103] International Trade Administration USA (2024), Vietnam - Power Generation, Transmission, and Distribution. https://www.trade.gov/country-commercial-guides/vietnam-power-generation-transmission-and-distribution (accessed 2 September 2024).

invested. EVN no longer hold monopoly on transmission and distribution of electricity.

- However, transmission is still dominated by EVN National Power Transmission Corporation (EVN NPTC). EVN NPTC is a state-owned transmission company that reports directly to EVN.
- As of Dec 2020, Viet Nam's transmission grid has 8,285km of 500kv transmission lines and 18,076km of 220kv transmission lines.
- For distribution, it is operated by the 5 subsidiaries of EVN (North Power Corp, Central Power Corp, South Power Corp, Hanoi Power Corp, HCM Power Corp). Each has a regional monopoly operation, and some regions have a commune operator. Implemented by each company's independent profit system. The distributors buy electricity from EVN NPTC to retail to end-consumers.

Trading Market:

- Wholesale segment started in Jan 2019 and is operated by the NLDC. Currently, 108 power plants are participating directly in it, with a capacity of over 30,837MW.
- Trading is done on spot market with ancillary services still in development.

Retail:

- Mainly operated by the five distribution companies under EVN with some operated by commune operators (electrification association, local government) that receives power from a power corporation.
- Electricity retailers must set up electricity selling prices based on the brackets of average electricity retail prices, the mechanism of price adjustment, and the structure of the electricity retail price list as provided by the Prime Minister.

100% FDI is allowed and there is no restriction concerning the foreign ownership of electricity companies or assets that are involved in electricity generation in Viet Nam. In Mar 2022, amendments to the Law on Electricity 2004 came into effect – private investors can:

(i) Invest in the construction of the electrical transmission grid; and

(ii) Operate the electricity transmission grid in which they are invested.

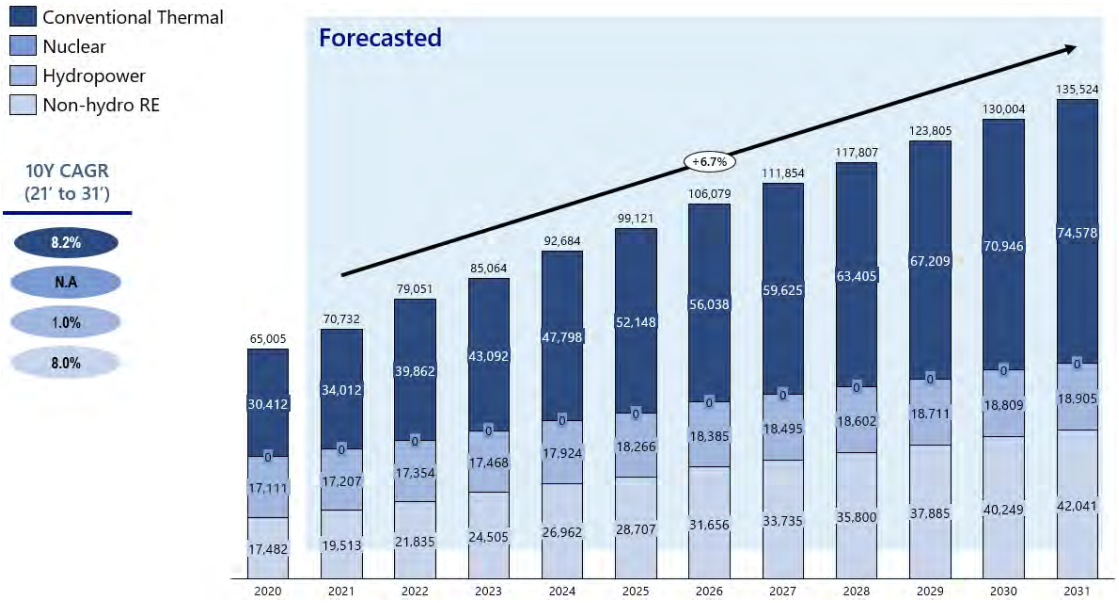
Renewable energy is also in the positive investment list that allows for 100% FDI[104].

Viet Nam's energy capacity is projected to reach 135,524 MW in 2031 at a CAGR of 6.7%. Conventional thermal power has the highest growth rate, followed by renewable energy

[104] Vietnam Briefing (2019), Renewables in Vietnam: Current Opportunities and Future Outlook. https://www.vietnam-briefing.com/doing-business-guide/vietnam/sector-insights/industry-spotlight-vietnam-s-renewable-energy-market (accessed 3 September 2024).

(not including hydropower).

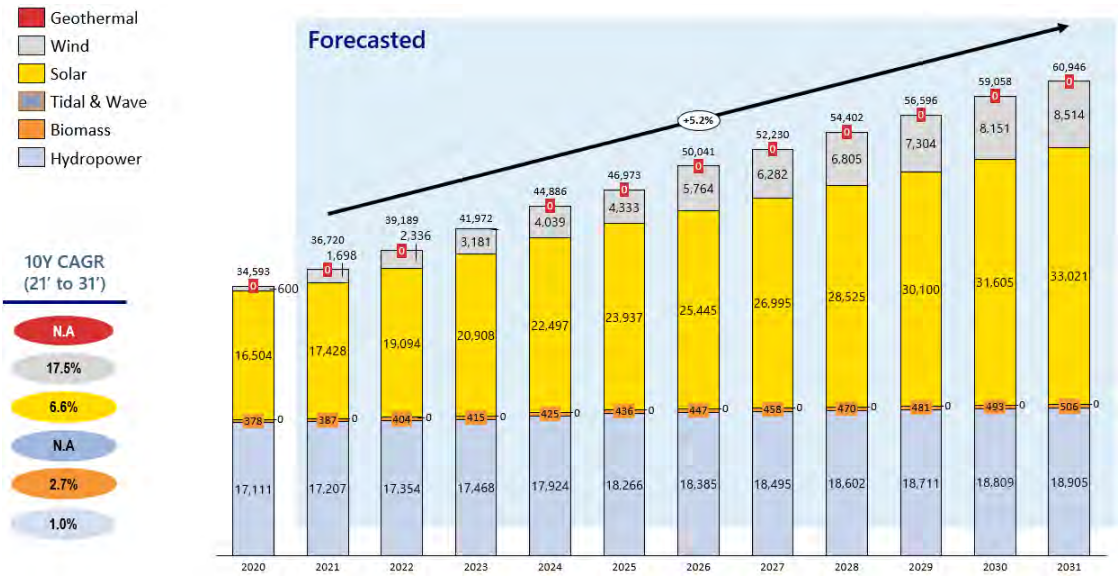
Figure A.31 Total Energy Mix Capacity (MW, 2023–2032F)



Source: Created by authorsbased on Fitch Solutions.

For renewable energy, solar PV and hydropower dominate, but wind power has the highest growth rate.

Figure A.32 Renewable Energy Mix Capacity (MW, 2023–2032F)



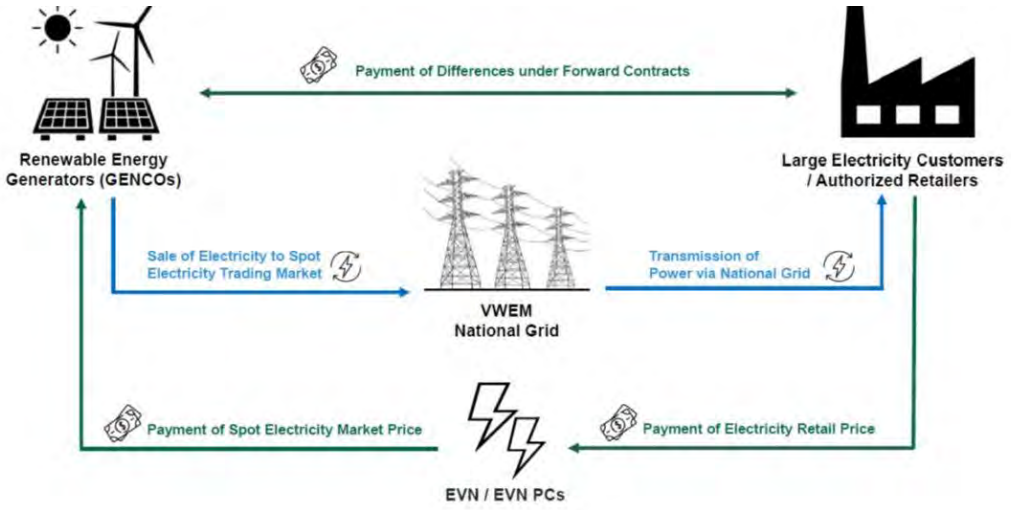
Source: Created by authors based on Fitch Solutions.

(2) Bilateral Trading

In Viet Nam, the Net-Metering scheme has been updated to follow a gross metering model since 2017 as it issued Decision No. 02/2019/QD-TTg which amends some points in Decision No. 11/2017/QD-TTg, which will change the trading method for rooftop solar projects by replacing the net-metering method with the direct consumption-direct supply method (gross metering). With the new method, buyers will now directly or separately pay for electricity they receive from rooftop project sellers. Sellers also need to directly pay for the electricity they receive and consume from the power grid. However, the net metering scheme has yet to be implemented as of 2023[105].

Other than the net-metering scheme, trading can occur between renewable energy developers and consumers through the Distributed Power Purchase Agreement (DPPA) system.

Figure A.33 DPPA Scheme (Grid-connected) in Viet Nam



Source: Lexology[106]

Under this scheme, the renewable energy developer sells the total electricity output to the wholesale market and earns revenue from the spot market. Additionally, the developer receives a pre-agreed renewable energy premium fee from the customer and provides the corresponding certificates to the customer. The physical delivery of electricity to the customer is facilitated by the electricity distribution retailer.

[105] ASEAN Energy Database Systems (n.d.), Vietnam abandons net-metering method for rooftop solar projects. https://aseanenergy.org/news-clipping/vietnam-abandons-net-metering-method-for-rooftop-solar-projects/ (accessed 5 September 2024).

[106] Lexology (2024), Launch of the Direct Power Purchase Mechanism in Vietnam. https://www.lexology.com/library/detail.aspx?g=f8ce4664-eed9-49b1-80f2-09879c57bbe7 (accessed 6 September 2024).

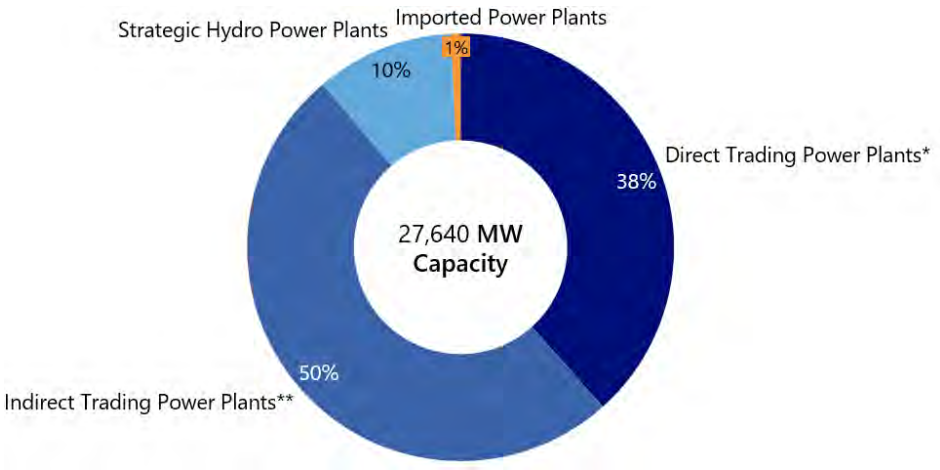
(3) Electricity Market Condition

In Viet Nam, there are wholesale market and capacity market but there is no voluntary carbon credit market or demand response programmes.

①Wholesale market

Formally introduced in 2019, the Vietnam Wholesale Energy Market (VWEM) has improved grid stability. Recent data indicates that 100 power plants directly participated in the wholesale electricity market with a total installed capacity of 27,640MW, accounting for 38% of the national power system[107].

Figure A.34 VWEM Generation installed capacity by market participation status (%) (2022)



Source: Created by authors based on EVN[108]

*Participants in VWEM which includes (i) grid-connected power plants with an installed capacity exceeding 30 MW, (ii) voluntary grid-connected power plants with an installed capacity below or equal to 30 MW; and (iii) non-hydropower renewable energy power plants with capacity exceeding 10 MW.

**These power plants do not have to participate directly in VWEM, and they sell power to EVNEPTC instead.

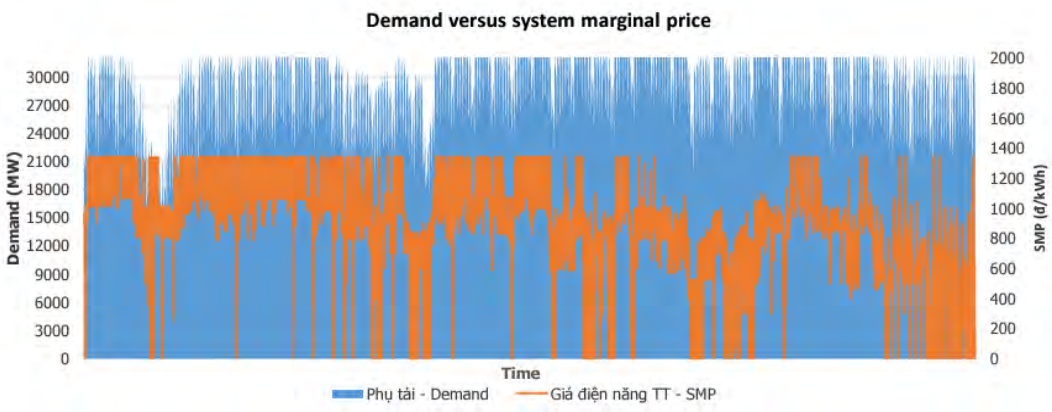
Prices in the wholesale market, which is referred to as the electricity sales price in the DPPA scheme system, vary between VND 0 and VND 1400, based on the diagram below,

[107] Baker McKenzie (2024), Vietnam: Draft new circular on the Vietnam wholesale electricity market's regulations and its implications for power projects. https://insightplus.bakermckenzie.com/bm/attachment_dw.action?attkey=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQJsWJiCH2WAWE%2FeOkjb67%2BkrsXbaIVGif&nav=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQbuwypnpZjc4%3D&attdocparam=pB7HEsg%2FZ312Bk8OIuOIH1c%2BY4beLEAe7RAboBpJzFs%3D&fromContentView=1 (accessed 9 September 2024).

[108] EVN (2024), Annual Report 2022 - 2023. Viet Nam. https://en.evn.com.vn/userfile/User/huongBTT/files/2024/5/EVNAnnualReport2022%202023.pdf (accessed 9 September 2024).

while demand fluctuated to as high as 21,000MW per hour.

Figure A.35 VWEM operational results (Hourly market price)



Source: EVN – NLDC, 2021[109]

②Ancillary Market

The ancillary service market is still in development as the incentive mechanism is still being tweaked. Due to poor incentive mechanism, there has been a lack of reserve to meet the uncertainty of renewables. As of 2023, the number of power plants participating in ancillary services (frequency response, fast start) is low.

Table A.6 VWEM's Current (2019) and Long-Term Targets

	VWEM (2019)	VWEM (Long-term target)
Trading Interval	60 minutes	30 minutes
Dispatch Interval	30 minutes	5 minutes
Ancillary Service	SMO will direct the regulation of power	Spot market with co-optimization energy bids and reserve bids
Settlement	SMO calculates invoices for EVN of bills for PCs and payments to generators	SMO does all spot market settlements for customers & generators
Price	Ex-post SMP	Ex-ante LMP

Source: Created by authors based on EVN – NLDC[110]

Note: SMO refers to 'System & Market Operator', SMP refers to 'System Marginal Price', PC refers to 'Power Corporations', and LMP refers to 'Locational Marginal Pricing'.

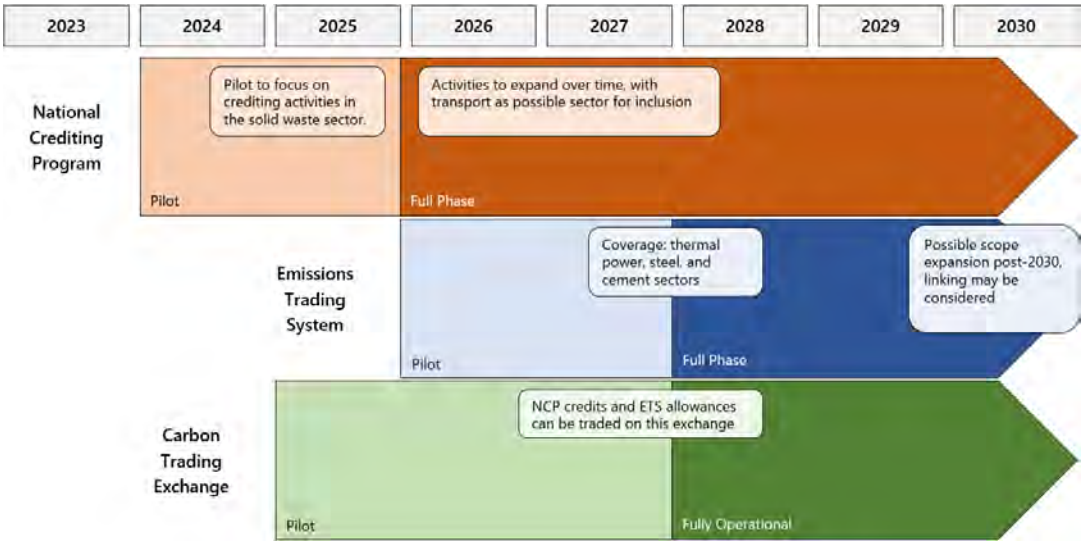
[109] EVN - NLDC (2021), VIETNAM WHOLESALE ELECTRICITY MARKET 2021. Viet Nam. https://vepg.vn/wp-content/uploads/2021/05/NLDC_VWEM-2021-22042021.pdf (accessed 9 September 2024).

[110] EVN - NLDC (2019), VIETNAM WHOLESALE ELECTRICITY MARKET (VWEM) OVERVIEW. Viet Nam. https://vepg.vn/wp-content/uploads/2019/09/3.-DPPA_VNWholesaleElecMarket_EVNNLDC_20190612_En.pdf (accessed 10 September 2024).

③Carbon Credit Market

There is no carbon credit market in Viet Nam but there are plans to establish and officially start its operations in 2028. The figure below shows the timeline on when and what activities will occur.

Figure A.36 Viet Nam's Domestic Carbon Market Timeline



Source: Created by authors based on various news articles.

④Demand Response Programmes

Although there are no demand response (DR) programmes, Viet Nam has recently undertaken a national-scale DR rollout to help maintain supply balance, quality and reliability, as well as to reduce the likelihood of potential supply shortages in the coming years.

Table A.8 Availability of DR Programmes in Viet Nam

Available	Unavailable (not yet introduced but can be implemented in future)
Non-Commercial DR In this model, there is no financial incentive. The reward can be a "advantage" in the form of preferential treatment if load curtailment is implemented as a last resort measure to maintain integrity of the power system.	**Curtailable Load Programme (CLP)** Targets industrial and commercial customers with flexible production lines and low to high consumption, fostering efficiency and cost reduction for the marginal unit of electricity.
Voluntary DR Programme In this model, there is no financial incentive. The reward may be in the form of goodwill as the customer is seen as contributing to social good.	**Emergency Demand Response Programme (EDRP)** Targets industrial and commercial customers with flexible production lines able to reduce electricity demand rapidly. This is deployed in event that the power system is overloaded.
	Non-dispatchable Time-based DR Programs (i) Two-tiered electricity tariff program – Comprising of demand charge and an energy charge. Customers can actively decide to adjust their demand to respond to price signals. (ii) Real-time peak-load electricity tariff program – Targeted at industrial and commercial customers. It includes a ToU tariff and a special tariff for peak time periods and is announced on a case-by-case by the operators.

Source: Created by authors based on Danish Energy Agency[111].

The table above shows a wide range of possibilities to participate in DR, from dispatchable and incentive-based programmes, to voluntary programmes according to circular 23 introduced by the government. However, as of 2022, only non-commercial and voluntary DR programmes have been introduced.

Thus far, two pilot projects were carried out as part of its national scale rollout, but they were implemented on a voluntary basis with very limited incentives and payments which saw overall low participation. Through the two DR pilot programmes, it was discovered that there was a need for better targeting of potential DR customers, as participation from industrial customers requires much higher incentives to compensate their potential revenue losses in shifting production processes. The Electronic Regulatory Authority of Vietnam (ERAV) concluded that the DR incentives that were offered were not sufficient as EVN Central Power Corporation (EVNCPC) allocated a limited amount of 20 million VND for each MW reduction, and the participants were only partly paid for their efforts to engage in DR.

Table A.9 Details on the Two DR Pilot Projects in Viet Nam

Year of Implementation	Details of pilot projects
2015	Two types of DR programmes were conducted under these pilot studies, Curtailable Load Programme (CLP) and Voluntary Emergency Demand Response Programme (VEDRP). Suitable customers are defined to be industrial and commercial customers who consume more than 1,000 MWh per year and who have electronic meters for remote data collection.
2019	EVN had instructed the National Load Dispatch Centre and Power Corporations (PC) to implement DR programmes under Circular 23 / 2017 / TT-BCT dated November 16, 2017 and Decision No. 54 / QDDTDL dated June 12, 2019 of the Ministry of Industry and Trade (MOIT) 2019 guiding DR implementation. NLDC and PCs had actively organized surveys, assessed DR potential, signed DR implementation agreements with customers, instructed PCs on non-commercial DR implementation process (DR agreement template, notification, verification of basic load routing, calculation of implementation results); developed demand response management software, completed, and applied at 5 PCs.

Source: Created by authors based on Danish Energy Agency[112].

[111] Danish Energy Agency (2022), Demand Response in Vietnam. https://ens.dk/sites/ens.dk/files/Globalcooperation/demand_response_in_vietnam_-_deliverable_2.1.pdf (accessed 10 September 2024).

[112] Danish Energy Agency (2022), Demand Response in Vietnam.

Following the conclusion of the pilot programmes, the government will implement more DSM and DR programmes to decrease the peak load capacity of the national power system by at least 1,500MW by 2025. This signal increasing emphasis on DR. To supplement DR, Viet Nam uses TOU mechanism to encourage market participants to lower their electricity consumption during peak hours, which may help lighten the grid load, but it is insufficient.

Table A.10 Viet Nam Wholesale Electricity Tariff (Industrial Zone and Market)

Voltage	Customer Group	Tariff (VND/kWh)
Voltage of 22kV and above	Standard hour	1,638
	Off-peak hour	1,064
	Peak hour	3,034
Voltage of 6kV up to below 22kV	Standard hour	1,697
	Off-peak hour	1,102
	Peak hour	3,132
Ref) Wholesale electricity tariff for market	-	2,562

Source: Created by authors based on EVN[113].

For years, the TOU mechanism has contributed to shifting demand toward off-peak hours. However, the difference between the time differentiated tariffs is not significant enough to attract DR implementation. Additionally, as the power system evolves, the definition of peak hours needs to be more dynamic to increase the efficiency of the TOU mechanism.

(4) Future opportunities for DES

According to the recently approved Viet Nam's Power Development Plan VIII (PDP8), it estimates that about 48% of Viet Nam's power supply will come from renewables by 2030, which far exceeded the target set by the Vietnam's National Energy Master Plan (NEMP) for renewables to account for 15 to 20% of Viet Nam's power supply by 2030. Hence, DES could play a role in the foreseeable future to promote grid stability arising from the growth in renewable energy[114].

https://ens.dk/sites/ens.dk/files/Globalcooperation/demand_response_in_vietnam_-_deliverable_2.1.pdf (accessed 10 September 2024).

[113] EVN (2023), WHOLESALE ELECTRICITY TARIFF. Viet Nam. https://en.evn.com.vn/d6/news/WHOLESALE-ELECTRICITY-TARIFF-9-28-260.aspx (accessed 11 September 2024).

[114] Green Finance & Development Center (2023), Vietnam's Eight National Power Development Plan (PDP8). https://greenfdc.org/vietnams-eight-national-power-development-plan-pdp8/ (accessed 15 September 2024).

1-1-7.Brunei

(1) Market Structure

Brunei Darussalam energy market is not liberalised. The government agency, the department of Electrical Services and Berakas Power Company Sdn Bhd (BPC) control the electricity generation, transmission and distribution in Brunei Darussalam.

Overview of the Electricity System in Brunei Darussalam

Regulatory Body[115]:

- Department of Energy regulates and oversees the development of petroleum-heavy energy sector in Brunei Darussalam. The role and responsibility of Department of Energy is Policy making and implementation of energy sector, ensuring stable supply of energy to the country.
- Specific to electricity sector, Department of Energy is supported by two agencies which are National Electricity Authority of Brunei Darussalam (AENBD) and the Department of Electrical Services (DES). AENBD focuses on strengthening the law and safety aspects of electricity in terms of generation, transmission and distribution. DES will perform the generation, transmission and distribution activities.

Generation:

- Government-related enterprises and agencies responsible for electricity generation in the country.
- Roughly 60% of electricity in the country is generated by Department of Electrical Services[116]. The remaining 40% of electricity is generated by Berakas Power Company Sdn Bhd (BPC).
- BPC is a government-linked company (GLC). BPC is a wholly owned subsidiary of Darussalam Assets Sdn, Bhd[117].

[115] ERIA (2021), Clean Electricity Supply: Temburong Ecotown Development Phase 4 pp.32-81. Jakarta. (accessed 19 September 2024).

[116] Berakas Power Company (2024), Core Business. Brunei Darussalam. https://www.bpc-brunei.com/aboutus/#core-business (accessed 24 July 2024).

[117] Ibid.

Transmission and Distribution[118]:

- Fully owned and operated by Department of Electrical Services (DES) and Berakas Power Company (BPC)
- DES power system covers Belait, Tutong District and supervises Temburong district (off-grid system). The transmission lines of DES power systems are 275 kV, 132 kV, and 66 kV.
- Berakas Power company covers Brunei Muara District. BP's transmission line is at 66 kV.
- The DES and BPC power systems are synchronised at 66kV transmission lines

Trading Market:

- There is no wholesale trading market in Brunei Darussalam. Like wholesale trading market, Brunei Darussalam does not have ancillary market service.

Retail:

- Department of Electrical Services and Berakas Power Company sell electricity directly to end consumer in each respective sector.

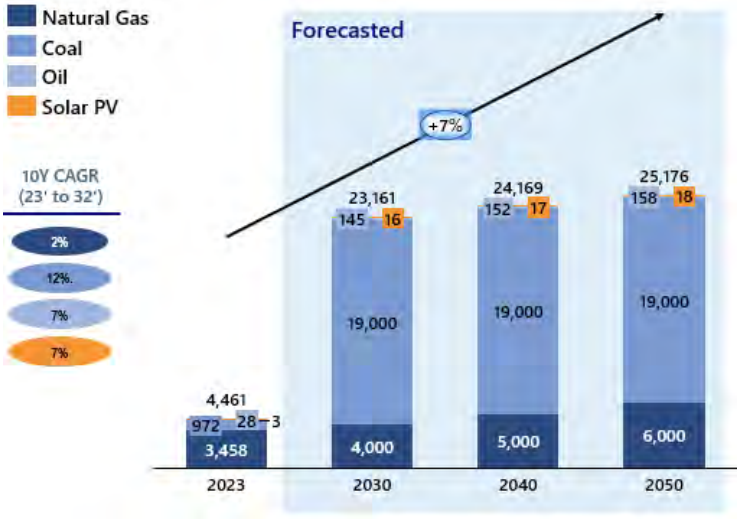
Although the energy market is not fully liberalised, 100% Foreign ownership of Renewable Energy companies are allowed in Brunei Darussalam. Renewable energy companies are fairly limited to EPC or technology providers to the government-linked companies or solar rooftop. However, under the Companies Act, at least two directors of the incorporated company must be a resident of Brunei Darussalam[119].

Furthermore, Brunei Darussalam Energy Production (GWh) is expected to increase from 4,461 GWh in 2023 to 25,176 GWh in 2050. This growth reflects a 7% CAGR from 2023 to 2050. The significant increase is attributed to the Government's plan to build coal power plants with generation capabilities of 19 GWh.

[118] ERIA (2021), Clean Electricity Supply: Temburong Ecotown Development Phase 4 pp.32-81. Jakarta. (accessed 19 September 2024).

[119] US Department of State (2020), 2020 Investment Climate Statements: Brunei. Washington, DC. https://www.state.gov/reports/2020-investment-climate-statements/brunei (accessed 19 September 2024).

Figure A.37 Total Energy Production GWh (2023–2050F)



Source: Created by authors based on Fitch Solutions.

Currently, roughly 77% of Brunei's electricity is generated from natural gas and 21% is generated from Coal. The remaining 2% are sourced from Oil and Solar. In terms of growth rate, electricity generation from coal has 12% CAGR from 2023 to 2050. Furthermore, the country plans to achieve 10% of renewable energy shares in the energy mix capacity by 2035. This resulted in a massive increase of solar electricity production with 7% CAGR from 2023 to 2050.

(2) Bilateral Trading

Brunei Darussalam's Ministry of Energy introduced Net-Metering Program in 2020 through numerous pilot projects. The pilot project took place in four residential houses and two government buildings.

In short, Brunei Darussalam's net metering scheme allows residential and commercial customers to sell its excess electricity, generated from Solar PV, to be sold back to the national grid. The net-metering programme allows residentials and commercial customers to sell 100% of its excess capacity to the national grid[120]. Brunei's four-tier electricity tariff is also applied in calculating the cost of electricity savings.

[120] Brunei Department of Energy (2022), Guidebook: Solar PV Rooftop and Net-Metering Programme. Brunei Darussalam. https://www.energy.gov.bn/Shared%20Documents/Resources/SOLAR%20PV%20GUIDEBOOK%20ENG.pdf (accessed 19 September 2024).

Table A.10 Brunei Darussalam Net Metering Scheme Calculation (Example)

Tier (kWh)	Tariffs per kWh	Electricity Generation (kWh)	Monetary value for savings
0 to 600	B$0.01	600 kWh	B$6
601 to 2000	B$0.08	307.2 kWh	B$24.58
2001 to 4000	B$0.10	-	-
Beyond 4001	B$0.12	-	-
Total		**907.2 kWh**	**B$30.58**

Source: Created by authors based on Department of Energy.

(3) Electricity Market Condition

There are no wholesale market and capacity market in Brunei Darussalam. Additionally, Corporate Purchase Agreement (CPPA) and Virtual Power Purchase Agreement (VPPA) are also not applicable in Brunei Darussalam. Currently, Brunei Darussalam is working on finalising carbon pricing and trading policies. The government is currently discussing an institutional framework for carbon trading and carbon policies on *Zero Routing Flaring* and *As Low As Reasonably Practicable* to reduce emissions from Industrial Sector. Furthermore, Carbon Pricing is included in Brunei Darussalam's National Climate Change Policy and the complete carbon-pricing instrument is expected to be launched by 2025. It is planned to be applicable to all industrial facilities emitting carbon beyond a carbon emissions limit threshold.

Other carbon trading, Brunei Darussalam is also working on establishing Renewable Energy Certificate Market. The International REC Standard Foundation board approved Brunei for I-REC for electricity issuance in June 2022. As of now, GCC is still the I-REC (E) issuer in Brunei until a suitable local organisation has been approved[121]. In February 2024, Brunei entered ASEAN bilateral meeting to address the gaps of REC market practice and seek potential alignment within BIMP (Brunei–Indonesia–Malaysia–Philippines). Lastly, The Department of Energy indicates that one RECs will be worth 1 MWh for renewable energy power, with the proposed fixed price at B$0.25 per kWh and B$250 per REC[122].

[121] The International Tracking Standard Foundation (2022), Brunei approved for I-REC(E) issuance. https://www.trackingstandard.org/brunei-approved-for-i-rece-issuance/ (accessed 8 August 2024).

[122] ASEAN-German Energy Programme (2016), RE Market in Brunei Darussalam. https://agep.aseanenergy.org/country-profiles/brunei-darussalam/brunei-re-sector/#1526611060469-668e6341-e2e4 (accessed 13 August 2024).

1-1-8.Cambodia

(1) Market Structure

Cambodia's energy market only allows private participation in power generation segment. In terms of transmission and distribution, Electricite du Cambodge (EDC) is still responsible. Rural Electricity Enterprises (REE) focuses on off-grid distribution where the locations are outside of the major cities.

Overview of the Electricity System in Cambodia

Regulatory Body[123]:

- Ministry of Mines and Energy (MME) is the policy maker (regulator) of electricity and energy development in Cambodia. This also includes energy mix planning and technical standards.
- In electricity sector, Ministry of Mines and Energy is supported by Electricity Authority of Cambodia (EAC) which focuses on enforcing regulation, electricity tariffs monitoring, overseeing permit licenses and financial performance of electricity business.

Generation[124]:

- Private Participation is allowed. Independent Power Producer plays a significant role in Cambodia's power generation.
- Private companies account for 88.5% and the remaining is coming from imports.
- EDC, a Cambodia State-owned electricity company, accounts for roughly 6.4% of Cambodia's power facility.

Transmission and Distribution:

- Private Participation is not allowed. Transmission and distribution are owned and operated by Electricite du Cambodia (EDC)
- EDC is responsible from distribution and transmission of electricity throughout Cambodia. It is concentrated mostly in Phnom Penh and provincial capitals.
- Off-Grid distribution, mostly outside of major cities, is handled by rural electricity enterprises (REEs) which can be private company or state-owned.

Trading Market:

- Cambodia does not have wholesale trading market and ancillary service market.

---

[123] OpenDevelopment Cambodia (2017), Electricity Infrastructure. Cambodia. https://opendevelopmentcambodia.net/topics/electricity-infrastructure (accessed 29 July 2024).

[124] ERIA (2017), Electric Power Policy and Market Structure in ASEAN Member States pp.3 -46. Jakarta. http ://www.eria.org/RPR_FY2015_No.18 _Chapter_2 .pdf, (accessed 23 July 2024).

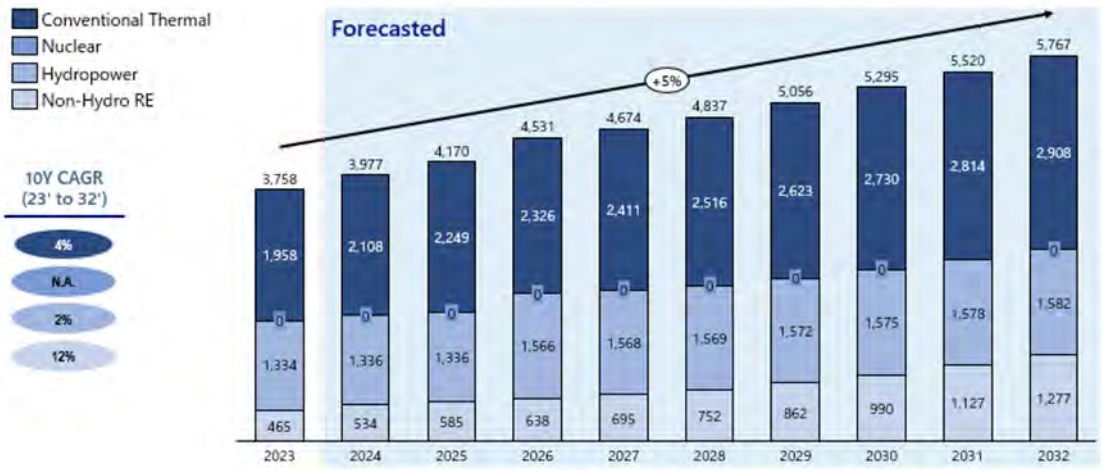
Retail:

- EDC sells the electricity directly to end-customers across major cities in Cambodia

Private sector plays a major role in the power generation sector of Cambodia. Furthermore, Green Energy is not on negative list of foreign direct investment sector, which allows for 100% ownership by foreign entities. The 100% FDI allowed since 2021 where the governing authority is the Council for the Development of Cambodia (CDC)[125].

The energy capacity of Cambodia is expected to grow from 3,758 MW in 2023 to 5,767 MW in 2032, which resulted in 5% CAGR. Non-Hydro Renewable category has the highest growth compared to all energy category, with 12% CAGR from 2023 to 2032. In terms of energy source, Hydro-based power still contributes around 52.9% of total energy generation.

Figure A.38 Total Energy Capacity MW (2023–2032F)

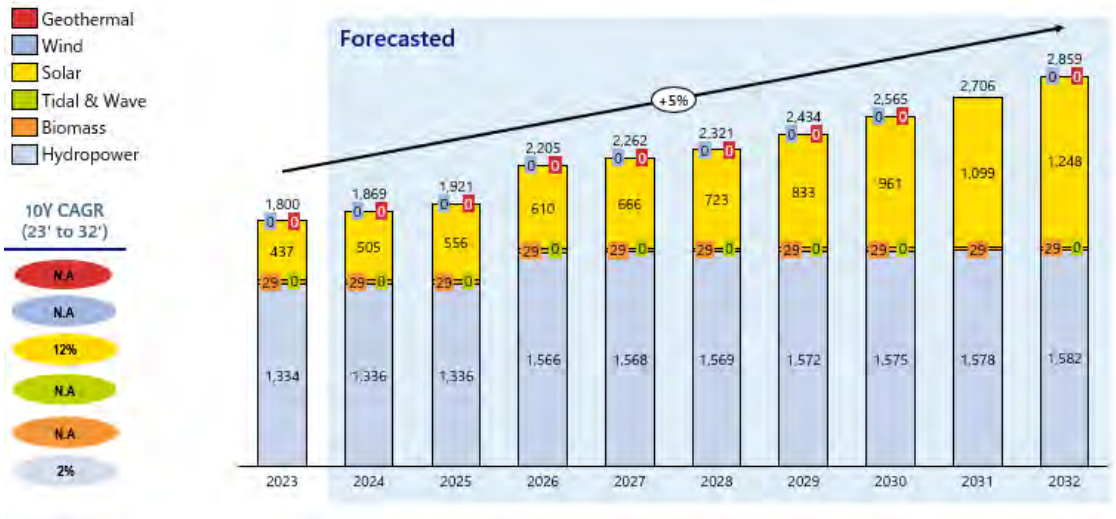


Source: Created by authors based on Fitch Solutions.

Solar PV has the highest growth across all renewable energy sources with 12% CAGR, while Hydropower has the slowest growth with 2% CAGR.

[125] OpenDevelopment Cambodia (2023), Foreign Investors. Cambodia. https://opendevelopmentcambodia.net/topics/foreign-investors/ (accessed 29 July 2024).

Figure A.39 RE Mix Capacity MW (2023–2032F)



Source: Created by authors based on Fitch Solutions.

(2) Bilateral Trading

As of now, Cambodia does not have any Net Metering Scheme or Net Billing.

(3) Electricity Market Condition

Wholesale electricity market, Corporate Purchase Power Agreement and Virtual Power Purchase Agreement (VPPA) are not permitted in Cambodia. In terms of carbon credit market, Cambodia does not have carbon credit market just yet, but it adopts Article 6 of the Paris Agreement to implement carbon credit mechanism. In December 2023, The Ministry of Environment of Cambodia had approved the Operations Manual for the implementation of Article 6 of the Paris Agreement on Climate Change[126].

1-1-9. Lao PDR

(1) Market Structure

Lao PDR adopts single-buyer marker for its energy market through Electricite du Lao (EDL). EDL is responsible for electricity generation, transmission and distribution in the country. Private participation plays a significant role in power generation segment, roughly 89% of electricity is generated from independent power plants.

Overview of the Electricity System in Lao PDR

[126] Dave Seibert-DFDL (2024), Cambodia: New Article 6 Regulations - Opportunities in the Carbon Credit Market. Cambodia. https://www.dfdl.com/insights/legal-and-tax-updates/cambodia-new-article-6-regulations-opportunities-in-the-carbon-credit-market/ (accessed 28 July 2024).

Regulatory Body[127]:

- The Ministry of Energy and Mines is responsible for policy development, strategy and management of energy and mining sectors.
- In electricity sector, MME is supported by Electricite du Laos (EDL) and Electrical Construction & Installation State Enterprise (ECI). EDL focuses on generation, transmission and distribution. Meanwhile, ECI focuses on construction of Lao PDR's energy infrastructure.

Generation[128]:

- Private Participation is allowed. Independent Power Producer plays a significant role in Lao PDR's power generation.
- EDL only accounts roughly for 10.7% of power generation, IPP accounts for 89.3%
- In terms of power generation, Lao PDR also imports electricity from EVN (Viet Nam) and EGAT (Thailand).
- EDL also exports some of its excess capacity to Thailand.

Transmission and Distribution:

- Transmission and distribution are owned and operated by EDL, Electricite du Laos.
- EDL is responsible from distribution and transmission of electricity in Lao PDR. In other words, EDL is a monopoly over power transmission and distribution

Trading Market:

- Lao PDR does not have wholesale electricity trading market and ancillary service market

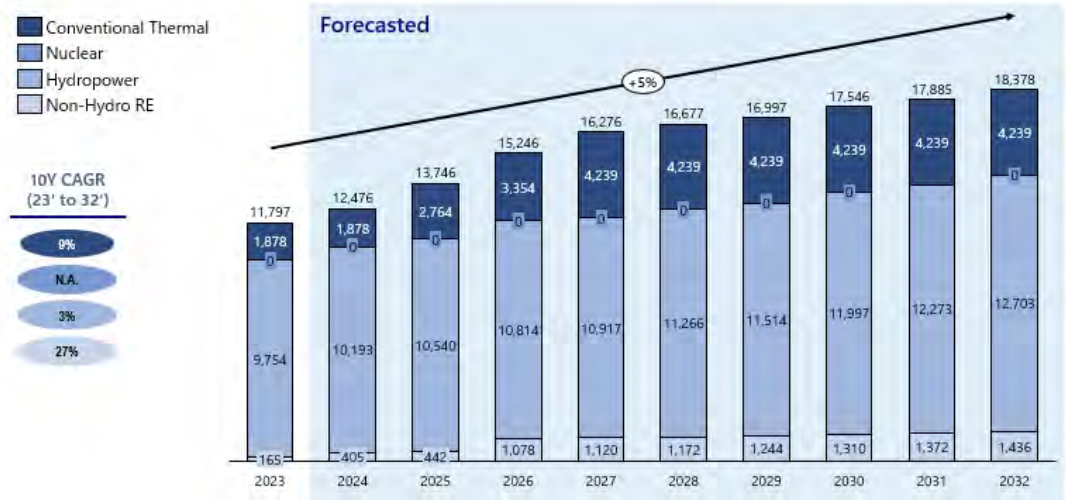
Retail:

- EDL sells the electricity directly to end-customers in Lao PDR.

[127] ERIA (2017), Electric Power Policy and Market Structure in ASEAN Member States pp.3–46. Jakarta. http ://www.eria.org/RPR_FY2015_No.18 _Chapter_2 .pdf, (accessed 23 July 2024).

[128] Ibid.

Figure A.40 Total Energy Mix Capacity MW (2023–2032F)



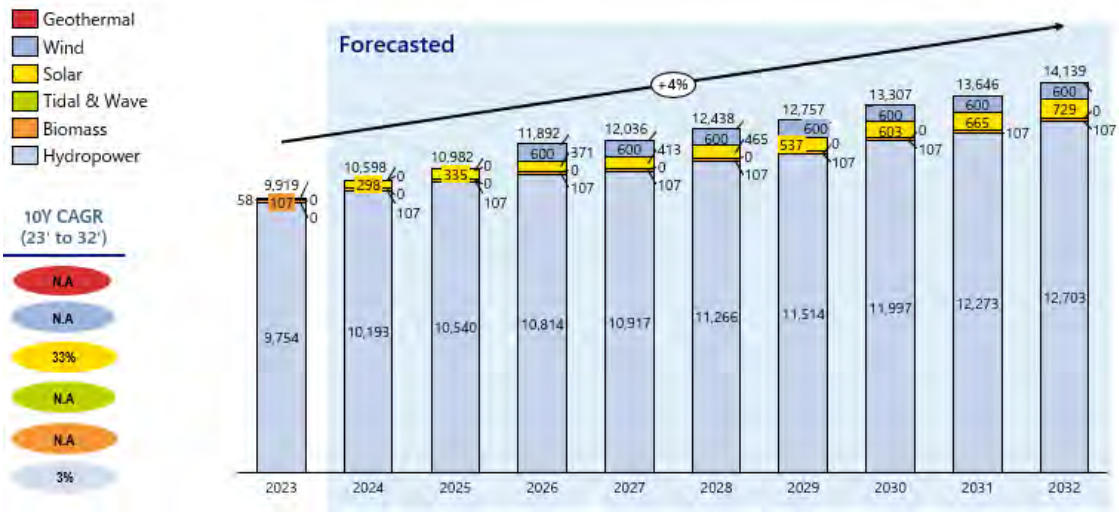
Source: Created by authors based on Fitch Solutions.

Lao PDR allows for full foreign ownership in renewable energy sector, except for small scale hydroelectric power.

Lao PDR allows for full foreign ownership in renewable energy sector, except for small scale hydroelectric power. The Electricity Law stated that there is a restriction of foreign capital injection into small-scale (Under 15 MW) hydroelectric power projects.

The energy capacity of Lao PDR is expected to increase from 11,797 MW in 2023 to 18,378 MW in 2032, which resulted in 5% CAGR. Hydropower is still the main energy source in Lao PDR with around 82% contribution in 2023.

Figure A.41 RE Mix Capacity MW (2023–2032F)



Source: Created by authors based on Fitch Solutions.

From the standpoint of renewable energy, Solar PV is expected to experience a high growth with 33% CAGR from 2023 to 2032.

(2) Bilateral Trading

As of now, there is no net metering scheme in Lao PDR. Net Metering Scheme is currently being prepared for Solar PV, specifically for NAMA-Rural Electrification Program. The current law does not cover financial options like net-metering of feed-in tariffs to improve investment or financial viability of small-scale energy projects.

In 2021, a grid-connected small-scale solar PV pilot (15 KWp), equipped with net metering capability, was installed to power the existing water pumping systems in Nouhak Phoumsavanh Public Park of Thamuang Village, Lao PDR[129].

(3) Electricity Market Condition

Corporate Power Purchase Agreement (CPPA) and Virtual Power Purchase Power Agreement (VPPA) are not applicable in Lao PDR. Carbon Credit Policy is still being developed by the government of Lao PDR through numerous initiatives. In May 2024, The Ministry of Natural Resources and Environment of Lao PDR along with the Government of Australia held a multi-stakeholder consultation on the decree of carbon credit in Lao PDR. The aim for this meeting is to address the issue around registration and management of carbon projects and its alignment towards the Paris Agreement[130]. Furthermore, Lao PDR government formed a collaboration with AIDC green forest, in launching a forest carbon credit initiative (REDD+) to reduce GHG emission from deforestation. The project is expected to reduce CO emission by 1.4 million tonnes annually[131]. Lastly, in June 2024, Lao PDR, represented by the Ministry of Natural Resources and Environment signed a memorandum of understanding (MoU) with Singapore on carbon credit collaboration.

1-1-10. Myanmar

(1) Market Structure

Energy Market in Myanmar is not fully liberalised. Private Participation is only allowed in power generation segment. Electricity Power Generation (EPGE) and Hydro Generation Enterprise (HPGE) buy electricity from independent power producer. EPGE is working

---

[129] Urban LEDS (2021), Lao Cities Pursue Low-Carbon Development with Solar Power and Energy Efficiency Projects. Lao PDR. https://urban-leds.org/lao-cities-pursue-low-carbon-development-with-solar-power-and-energy-efficiency-projects/ (accessed 29 July 2024).

[130] GGGI (2024), Government of Lao PDR holds multi-stakeholder consultation on the draft Decree on Carbon Credits. Lao PDR. https://gggi.org/government-of-lao-pdr-holds-multi-stakeholder-consultation-on-the-draft-decree-on-carbon-credits/ (accessed 21 August 2024).

[131] The Laotian Times (2024), Laos Launches Forest Carbon Credit Initiative to Combat Climate Change. Lao PDR. https://laotiantimes.com/2024/05/09/laos-launches-forest-carbon-credit-initiative-to-combat-climate change. (accessed 19 August 2024).

under The Department of Electric Power and Planning. Meanwhile, HPGE is under Department of Hydropower.

Overview of the Electricity System in Myanmar

Regulatory Body[132]:

- The Ministry of Electric Power (MEP) focuses on policy development, planning and monitoring of power generation, transmission and distribution of electricity in Myanmar. MEP is part of National Energy Management Committee (NEMC).
- In electricity sector, MEP is supported by Department of Power Transmission and Control, Department of Electric Power and Planning, Department of Hydropower Implementation.

Transmission and Distribution:

- EPGE is responsible for transmission in Myanmar.
- In terms of distribution, Electricity distribution in Myanmar is operated by YESC, MESC and ESE. Yangon Electricity Supply Corporation (YESC) is responsible for electricity supply in Yangon District. Mandalay Electricity Supply Corporation (MESC) is responsible for supply in Mandalay District. Electricity Supply Enterprise (ESE) is responsible for supply in districts except Mandalay and Yangon.

Trading Market:

- Myanmar does not have wholesale electricity market and ancillary service market.

Retail:

- In retail sector, YESC, MESC and ESE sell electricity directly to end-consumers in their respective customers.

Renewable energy generation (IPPs) is applicable for 100% of foreign ownership. 100% foreign ownership is allowed since 2016 by the Myanmar Investment Commission[133].

Renewable energy, specifically Hydropower, plays significant role in Myanmar's power generation, accounting for 46% of energy mix in 2023, while Non-Hydro RE only accounts for 2%–3%. The overall growth of energy capacity in Myanmar is at 2% CAGR from 2023 to 2032.

---

[132] ERIA (2017), Electric Power Policy and Market Structure in ASEAN Member States pp.3 -46. Jakarta. http ://www.eria.org/RPR_FY2015_No.18 _Chapter_2 .pdf , (accessed 23 July 2024).

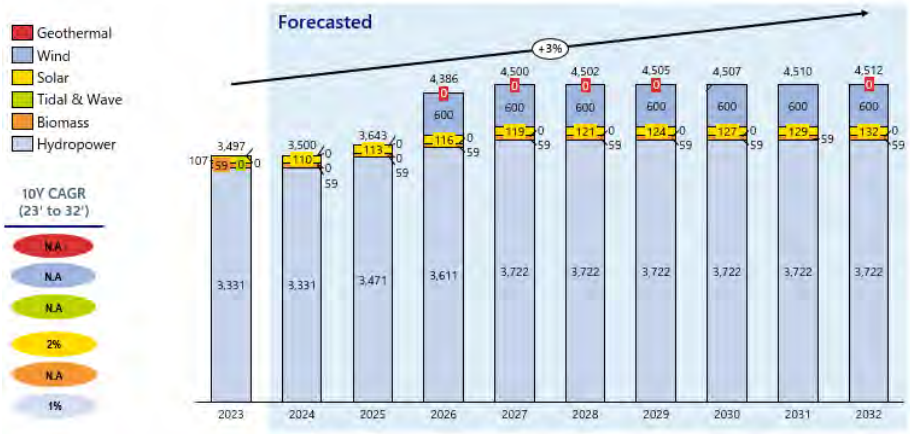
[133] Directorate of Investment and Company Administration (2017), The Notification No.15/20187 on the List of Restricted Investment Activities. Myanmar. https://www.dica.gov.mm/en/news/announcement-notification-list-restricted-investment-activities (accessed 30 July 2024).

Figure A.42 Total Energy Mix Capacity MW (2023–2032F)

Source: Created by authors based on Fitch Solutions.

Solar PV has a slightly higher growth compared to other RE sources with 2% CAGR from 2023 to 2032.

Figure A.43 RE Mix Capacity MW (2023–2032F)



Source: Created by authors based on Fitch Solutions.

(2) Bilateral Trading

As of now, Myanmar does not have specific policy for rooftop solar business as well as net metering scheme.

(3) Electricity Market Condition

Corporate Power Purchase Agreement (CPPA), Virtual Power Purchase Agreement (VPPA) and Carbon Credit are not applicable in Myanmar. In terms of carbon credit, the government of Myanmar is still focusing on developing the overall measurement, reporting and verification framework.

1-2. Country Overview of Cybersecurity Issues and Cybersecurity for Distributed Energy Systems in ASEAN

1-2-1. Singapore

(1) Overview on Cybersecurity

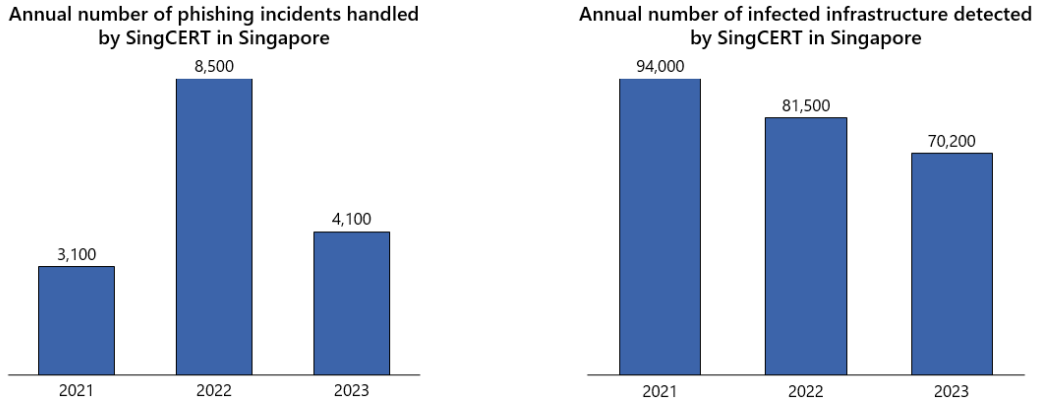
The number of phishing cases mirror global trends, as phishing remains one of the most popular and effective threat vectors. The annual number of phishing incidents handled by the Singapore Cyber Emergency Response Team (SingCERT) under the Cyber Security Agency of Singapore (CSA) was 3,100 in 2021. It more than doubled to about 8,500 incidents in 2022, but dropped back down to 4,100 in 2023.

On the other hand, the number of infected infrastructure declined steadily between 2021 to 2023, indicating an overall improvement in cyber hygiene levels. The annual number of infected infrastructure was initially 94,000 in 2021, but it decreased to 70,200 in 2023.

According to the CSA, threat actors are increasingly leveraging AI chatbots to improve the quality of their phishing emails. As such, relying on the ability to spot bad grammar or typo errors, which are the typical tell-tale signs of phishing, may not be sufficient anymore.

As for the improvement in cyber hygiene (and the corresponding decrease in the number of infected infrastructure), the overall number of infected systems still remains high due to the use of dated cybersecurity protection software and the lack of awareness of good cyber practices amongst individuals and businesses.

Figure A.44 Overview of Cybersecurity in Singapore



Source: Created by authors based on CSA[134].

[134] CSA (2024), Singapore Cyber Landscape 2023. https://www.csa.gov.sg/Tips-Resource/publications/2024/singapore-cyber-landscape-2023 (accessed 3 October 2024).

CSA (2023), Singapore Cyber Landscape 2022. https://www.csa.gov.sg/Tips-Resource/publications/2023/singapore-cyber-landscape-2022 (accessed 3 October 2024).

Table A.11 Notable Cases of Cyberattacks on the Public Sector in Singapore

Type of DES	Type of attack	Year	Incident	Overview	Impact
-	DDoS	2023	Disruption of public healthcare institutions' websites	In November 2023, national health technology provider Synapxe, which supports the operations of 46 public healthcare institutions including hospitals and polyclinics, had its servers flooded with internet traffic.	There was no indication that public healthcare data and internal networks were compromised. However, the attack caused a seven-hour disruption, preventing access to websites, emails, and productivity tools.
-	Data Breach	2017	Personal details of 850 national servicemen and staff at the Ministry of Defence were stolen	In February 2017, it was discovered that the Ministry of Defence's internet system was breached. Investigations indicated that the real purpose may have been to gain access to official secrets, Furthermore, it was suspected that the attack could have been state sponsored.	The stolen data from the 850 victims included personal information such as national identification numbers, telephone numbers, and dates of birth. However, due to physical separation from internal systems, no classified military information or operational data was exfiltrated.

Source: Created by authors based on various news articles[135].

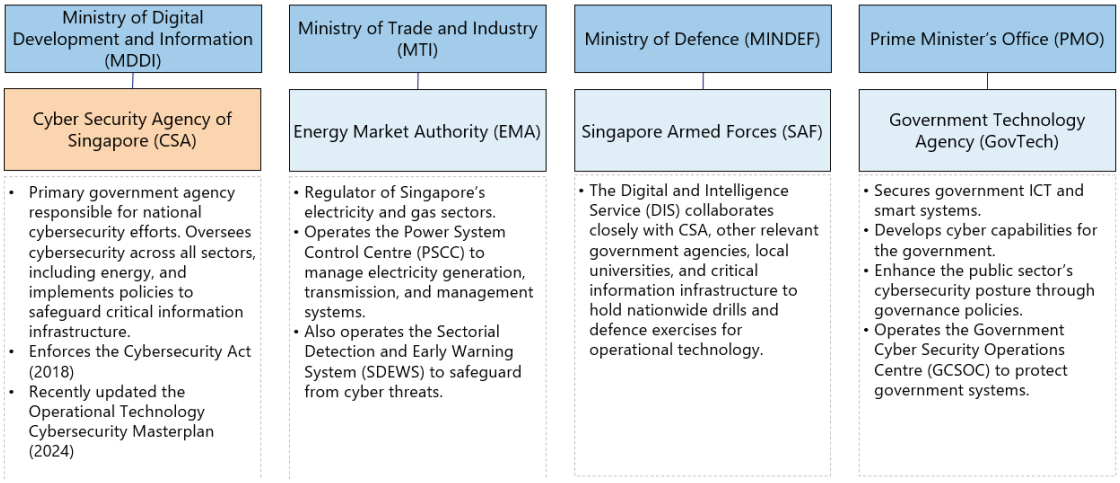
(2) Government Structures related to Cybersecurity for DES

There are four main government agencies in charge of cybersecurity policies for the energy sector in Singapore – namely the Cyber Security Agency of Singapore (CSA) under the Ministry of Digital Development and Information (MDDI), the Energy Market Authority (EMA) under the Ministry of Trade and Industry (MTI), the Singapore Armed Forces, and GovTech.

[135] Today Singapore (2023), Cyberattack caused 7-hour internet outage that hit public hospitals, polyclinics; attacks continuing: Synapxe. https://www.todayonline.com/singapore/cyberattack-caused-7-hour-internet-outage-hit-public-hospitals-polyclinics-attacks-continuing-synapxe-2297036 (accessed 3 October 2024).

The Straits Times (2017), Personal data of 850 national servicemen and Mindef staff stolen in targeted cyber attack. https://www.straitstimes.com/singapore/personal-data-of-850-mindef-servicemen-and-staff-leaked-due-targeted-planned-cyber-attack (accessed 3 October 2024).

Figure A.45 Overview of Government Structures related to Cybersecurity for DES



Source: CSA[136], EMA[137], MINDEF[138], GovTech[139].

(3) Policies on Cybersecurity for DES

There are numerous government policies and initiatives for nationwide and cross-sector cybersecurity. Specifically, the CCoP, OT Cybersecurity Masterplan 2024, and CLS are relevant to cybersecurity for the energy sector.

[136] CSA (2024), What We Do. https://www.csa.gov.sg/Explore/what-we-do (accessed 3 October 2024).

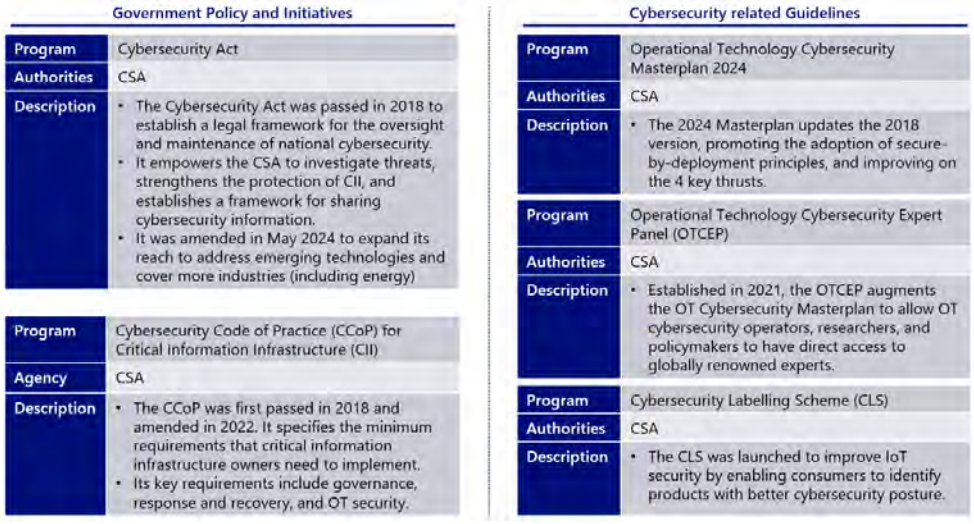
[137] EMA (2024), Our Role as a Power System Operator. https://www.ema.gov.sg/about-ema/who-we-are/our-role-as-a-power-system-operator (accessed 3 October 2024).

[138] MINDEF (2022), National Agencies Tackle Cyber Threats at Inaugural Cyber Defence Exercise; DIS and CSA Sign Joint Operations Agreement for Cyber Cooperation. https://www.mindef.gov.sg/news-and-events/latest-releases/16nov22_nr (accessed 3 October 2024).

[139] GovTech (2024), Safeguarding the Government's Information and Communications Technology & Smart Systems. https://www.tech.gov.sg/our-capabilities/cybersecurity/ (accessed 3 October 2024).

GovTech (2023), Factsheet – Government Cyber Security Operations Centre (GCSOC). https://www.smartnation.gov.sg/media-hub/press-releases/gcsoc-factsheet/ (accessed 3 October 2024).

Figure A.46 Overview of Government Policies, Initiatives, and Guidelines related to Cybersecurity for DES in Singapore



Government Policy and Initiatives

Program	Cybersecurity Act
Authorities	CSA
Description	• The Cybersecurity Act was passed in 2018 to establish a legal framework for the oversight and maintenance of national cybersecurity. • It empowers the CSA to investigate threats, strengthens the protection of CII, and establishes a framework for sharing cybersecurity information. • It was amended in May 2024 to expand its reach to address emerging technologies and cover more industries (including energy)

Program	Cybersecurity Code of Practice (CCoP) for Critical Information Infrastructure (CII)
Agency	CSA
Description	• The CCoP was first passed in 2018 and amended in 2022. It specifies the minimum requirements that critical information infrastructure owners need to implement. • Its key requirements include governance, response and recovery, and OT security.

Cybersecurity related Guidelines

Program	Operational Technology Cybersecurity Masterplan 2024
Authorities	CSA
Description	• The 2024 Masterplan updates the 2018 version, promoting the adoption of secure-by-deployment principles, and improving on the 4 key thrusts.

Program	Operational Technology Cybersecurity Expert Panel (OTCEP)
Authorities	CSA
Description	• Established in 2021, the OTCEP augments the OT Cybersecurity Masterplan to allow OT cybersecurity operators, researchers, and policymakers to have direct access to globally renowned experts.

Program	Cybersecurity Labelling Scheme (CLS)
Authorities	CSA
Description	• The CLS was launched to improve IoT security by enabling consumers to identify products with better cybersecurity posture.

Source: Created by authors based on CSA[140].

The key policy initiative related to cybersecurity for DES is the Operational Technology Cybersecurity Masterplan. The inaugural Masterplan was launched in 2019, when OT cybersecurity in Singapore's essential service sectors was still at an early stage. Back then, the aim was to create awareness for the challenges faced by the OT community, align efforts of OT stakeholders, and strengthen partnerships to drive OT cybersecurity initiatives and address emerging OT cyber threats.

There are four key thrusts in the Masterplan:

1. OT Cybersecurity Training
2. OT Cybersecurity Information Sharing and Analysis Centre (OT-ISAC)
3. Strengthening Policies and Processes
4. Adopting Technologies for Cyber Resilience

---

[140] CSA (2024), Cybersecurity Act. https://www.csa.gov.sg/legislation/Cybersecurity-Act (accessed 3 October 2024).

CSA (2022), Cybersecurity Code of Practice for Critical Information Infrastructure - Second Edition. https://www.csa.gov.sg/docs/default-source/legislation/ccop_second-edition.pdf?sfvrsn=b2ab666a_2 (accessed 3 October 2024).

CSA (2024), Singapore's Operational Technology Cybersecurity Masterplan 2024. https://www.csa.gov.sg/Tips-Resource/publications/2024/operational-technology-cybersecurity-masterplan-2024 (accessed 3 October 2024).

CSA (2024), Operational Technology Cybersecurity Expert Panel. https://www.csa.gov.sg/Explore/who-we-are/committees-and-panels/operational-technology-cybersecurity-expert-panel (accessed 3 October 2024).

CSA (2024), Cybersecurity Labelling Scheme (CLS). https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme (accessed 3 October 2024).

Figure A.47 Four Key Thrusts of Singapore's OT Cybersecurity Masterplan 2019 and 2024

Source: CSA[141].

Table A.12 Achievements and Updates in Singapore's OT Cybersecurity Masterplan 2024

Key Thrust 1: OT Cybersecurity Training	
Achievements so far	• Trained 400 OT cybersecurity professionals since 2019. • Launched the OT Cybersecurity Competency Framework (OTCCF) to identify relevant career pathways and competencies required to attract, train, and develop talent for the OT ecosystem.
Updates in 2024 Masterplan	Improve OT cybersecurity professional competency and pipeline • Address the lack of OT cybersecurity manpower, especially for SMEs. • Incorporate OT cybersecurity syllabus into mandatory modules for university computer science and engineering courses.
Key Thrust 2: OT Cybersecurity Information Sharing and Analysis Centre (OT-ISAC)	
Achievements so far	• Launched the OT-ISAC together with the Global Resilience Federation Asia-Pacific in 2019. • Partnered with threat intelligence agencies and Cyber Emergency Response Teams (CERTs) to promote the sharing and adoption of OT cybersecurity best practices.
Updates in 2024 Masterplan	Enhance information sharing and reporting • Streamline information sharing mechanisms to enhance collaboration with CII sector regulators. • Create a system to offer protection from liability to encourage businesses to come forward and report and share threat info.

[141] CSA, Singapore's Operational Technology Cybersecurity Masterplan 2024.

Key Thrust 3: Strengthening Policies and Processes	
Achievements so far	• Issued the Cybersecurity Code of Practice (CCoP), which prescribes implementation requirements for critical information infrastructure owners, in 2018.
Updates in 2024 Masterplan	Uplift OT cybersecurity resilience beyond the CII • Update existing guidelines to include non-CII sectors. • Prioritise consequences management in the design and operation of OT systems to include wider supply chain risks. • Adapt best practices for use in the non-CII environment.
Key Thrust 4: Adopting Technologies for Cyber Resilience	
Achievements so far	• Launched the Cybersecurity Industry Call for Innovation (CyberCall) programme in 2018 to promote the development of cutting-edge cybersecurity solutions to meet both national and commercial needs. • Funded more than S$20 million for 12 OT cybersecurity projects which include power transmission, autonomous vehicles, and onboard vessel systems. • Launched the National Cybersecurity Research and Development Programme (NCRP) to drive innovation through a whole-of-government approach.
Updates in 2024 Masterplan	Establish an OT cybersecurity centre of excellence and promote secure-by-deployment throughout the life cycle of the OT system • Collaborate with OEMs and solution partners to establish an OT cybersecurity centre of excellence to simulate real world cybersecurity testing. • Work with all relevant stakeholders to incorporate 'secure-by-deployment' principles from product design, configuration, deployment and maintenance.

Source: Created by authors based on CSA[142]

(4) Guidelines on Cybersecurity for DES

In the Operational Technology Cybersecurity Masterplan 2024, 'Secure-by-Deployment' is a concept that is referred to several times. It is one of, if not the most important update to the 2018 Masterplan. This concept seeks to refresh the thought process behind OT cybersecurity by securing the entire life cycle management of OT systems instead of carrying out piecemeal cybersecurity initiatives. This is because OT systems usually consist of multiple products from different OEMs, which are assembled by different system integrators and operated by the asset owners.

[142] ibid.

Figure A.48 Secure-by-Deployment Principles in the OT Cybersecurity Masterplan 2024

Stakeholder	Role
OEM	• Ensure that their products are secure-by-design • Incorporate the best practices across the industry to mitigate cyber threats upfront and throughout the products' life cycle • Also need to ensure that they deliver products or systems which are secure-by-default, keeping in mind the complexities and costs which users may potentially face • Ensure that security patches or updates are made available to the users
System integrator	• Employ qualified personnel who are trained to configure the OT equipment in accordance with the OEM's specifications • Install the OT equipment securely
OT asset owner	• Ensure that security patches or updates are installed on a timely basis • Continuously monitor the security state of the deployed OT asset and take care not to introduce cyber risks to the OT system • Also need to continuously engage the OEMs and system integrators to ensure that the OT system is adequately secured throughout its life cycle.

Source: Created by authors based on CSA[143]

The Cybersecurity Code of Practice (CCoP) for CII was first launched by the CSA in 2018, and it was updated to its current version (CCoP 2.0) in 2022. It specifies the minimum requirements that critical information infrastructure owners need to implement to ensure the cybersecurity of their assets. It also has legal effect, and CII owners are obliged to ensure full compliance with it under the Cybersecurity Act. There are nine key requirements as shown in the table below.

Table A.13 Cybersecurity Code of Practice (CCoP) for Critical Information Infrastructure

Key Requirements	Description
1. Audit	• Weaknesses and vulnerabilities found in audit findings need to be prioritised and remediated in a timely manner depending on their severity. • Establishment of a clear timeline to implement these remediation actions.
2. Governance	• Adequate resources and attention must be devoted to the CII owner's cybersecurity strategy and its application to the assets. • A clear organisational structure and cybersecurity risk management framework needs to be established and implemented. • Policies, standards, guidelines, and procedures need to be put in place to reduce uncertainty and simplify complexity. • Adequate processes must be put in place for change management, use of cloud computing systems, and outsourcing and vendor management.

[143] ibid.

3. Identification	• Establishment of mechanisms to identify all CII assets and maintain an inventory of these assets.
4. Protection	• The CII owner should carry out access control and account management to prevent unauthorised access to protected systems. • Network segmentation and network security should also be established to restrict and prevent traversal of malicious actors. • Adequate measures need to be in place for remote connection, wireless communication, portal devices, and removable media.
5. Detection	• Logging and monitoring of traffic and activities to detect potential threats. • Carrying out of proactive threat hunting and cyber threat information sharing with other parties.
6. Response and Recovery	• Minimise the impact of cybersecurity incidents through incident management and a crisis communication plan. • The CII owner should also carry out periodic cybersecurity exercises to assess and validate their cybersecurity capabilities.
7. Cyber Resiliency	• Establishment of plans for backup and restoration, as well as business continuity.
8. Cybersecurity Training & Awareness	• Carry out adequate cybersecurity awareness improvement programmes and training courses to equip employees with the required knowledge and skills to perform their roles and responsibilities effectively.
9. OT Security	• Ensure that the OT environment is separated from the IT environment where possible, and data flow is restricted. • Implement security mechanisms and processes to ensure secure coding and protect field controllers.

Source: Created by authors based on CSA[144]

(5) Initiatives or Case Studies on Cybersecurity for DES

CSA actively engages industry experts and stakeholders from different countries and from different parts of the OT cybersecurity value chain through the Operational Technology Cybersecurity Expert Panel (OTCEP). Established in 2021, the OTCEP supports efforts under the OT Cybersecurity Masterplan and improves cross-sector response to mitigate cyber threats in the OT environment. It is made up of a diverse group of experts, including OT cybersecurity practitioners, CII asset operators, industry stakeholders, researchers, and policymakers from different backgrounds and countries.

The CSA is the main organiser of the OTCEP. It invites global experts to be members of the OTCEP and organises annual events for it. Furthermore, OTCEP members are shortlisted

[144] CSA, Cybersecurity Code of Practice for Critical Information Infrastructure.

based on their OT experience, and they come from both public and private sectors. There are currently 10 OTCEP 2024 members, and they include members from the US, Europe (Germany), and Asia (Kazakhstan, Singapore, and Taiwan).

At the OTCEP events, key topics such as global OT technologies, emerging cyber threats, experience in handling global cybersecurity incidents, talent capacity building, and best practices are discussed by these experts.

Figure A.49 Operational Technology Cybersecurity Expert Panel (OTCEP) 2024

Source: CSA[145]

On the other hand, the CSA has also worked on an initiative for consumers. It created a scheme known as the Cybersecurity Labelling Scheme (CLS) for consumer smart devices, as part of efforts to enhance IoT security and improve overall cyber hygiene levels. The CLS is similar to the scheme for energy labels, with a tiered reference to security levels that will serve as a guide for consumers to make informed decisions.

Currently, Singapore has signed mutual recognition agreements with Finland and Germany. In 2024, CSA signed a mutual recognition agreement with the Connectivity Standards Alliance for the recognition of their respective cybersecurity labels for consumer IoT devices. There are plans to sign more mutual recognition agreements with other countries and expand the adoption of these standards.

These mutual recognition agreements help harmonise standards, reduce redundant testing and costs for manufacturers, promote the exchange and alignment of information on relevant standards and requirements, and encourage collaboration on the continued development of respective cybersecurity certification and labelling schemes.

[145] CSA, Operational Technology Cybersecurity Expert Panel.

CSA (2024), 2024 OTCEP Members. https://www.otcep.gov.sg/2024-otcep-members/ (accessed 3 October 2024).

Figure A.50 Cybersecurity Labelling Scheme (CLS)

Source: Created by authors based on CSA[146]

1-2-2. Philippines

(1) Overview on Cybersecurity

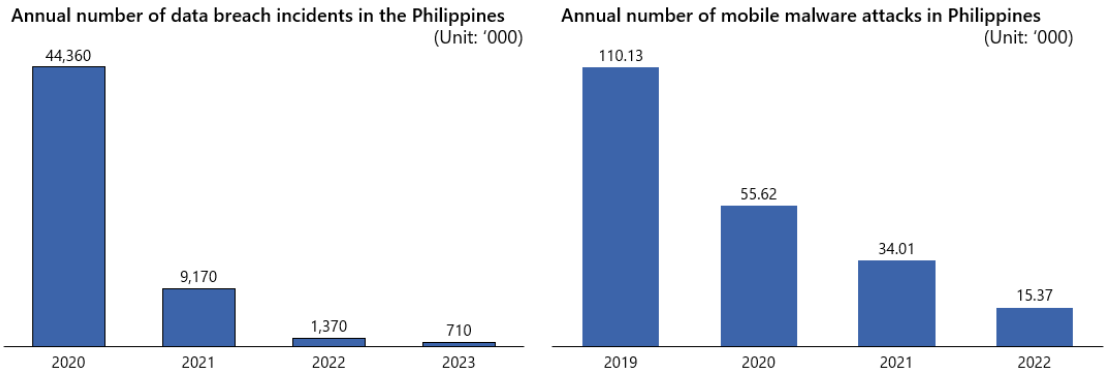
Both the number of data breach incidents and mobile malware attacks decreased over the past few years in the Philippines, suggesting that cybersecurity initiatives are taking effect in preventing cyberattacks. Philippines was cited as the 16th most breached country in between 2004 to present time. Over time, there has been a decrease in the number of data breaches. The decrease was most significant between 2020 and 2021, where the number of annual data breach incidents decreased from 44.36 million to 9.17 million[147]. Similarly, the number of mobile malware attacks in the Philippines has also been decreasing year-on-year. The decrease was between 2019 and 2022, where the number of mobile malware attacks halved from approximately 110,000 to approximately 15,000[148].

[146] CSA, Cybersecurity Labelling Scheme.

[147] Statista (2024), Number of incidents of data breaches in the Philippines from 1st quarter 2020 to 4th quarter 2023. https://www.statista.com/statistics/1271333/philippines-number-of-data-breaches/ (accessed 30 July 2024).

[148] Statista (2024), Number of mobile malware attacks detected in the Philippines from 2019 to 2022. https://www.statista.com/statistics/1277044/philippines-number-of-foiled-mobile-malware/ (accessed 30 July 2024).

Figure A.51 Overview of Cybersecurity in the Philippines



Source: Statista[149]

There were no notable cyberattacks specifically related to DES in the Philippines. However, some have attributed the numerous power and internet outages to the involvement of China's State Grid Corporation due to its involvement in the National Grid Corporation of the Philippines[150]. Separately, there was an attack on one of the Department of Energy's websites[151].

Table A.14 Notable Cases of Cyberattacks on DES in the Philippines

Year	Incident	Overview	Impact
Last few years	Potential foreign intervention in the national grid	China's State Grid Corporation owns a 40% share in the National Grid Corporation of the Philippines, leading to allegations of foreign control. Also, **allegations of engineered power and internet outages have been attributed to the Chinese government.**	As a result of these allegations, the Philippines government commissioned a cybersecurity audit team consisting of officials from the National Security Council and the armed forces to assess various sites and **make periodic cybersecurity assessments.**
2024	Department of Energy had one of its websites hacked	The Government Energy Management Program (GEMP) website of the Department of Energy (DOE) was hacked and defaced.	The authorities took the system offline and coordinated with the Philippine National Computer Emergency Response Team (NCERT) and the system developer to address the vulnerabilities of the website.

Source: ASEAN Energy Database System, GMA Integrated News.

[149] Statista (2024), Number of incidents of data breaches in the Philippines from 1st quarter 2020 to 4th quarter 2023.

[150] ASEAN Energy Database System (2020), Philippines steps up security to shield power grid from foreign control. https://aseanenergy.org/news-clipping/philippines-steps-up-security-to-shield-power-grid-from-foreign-control/ (accessed 30 July 2024).

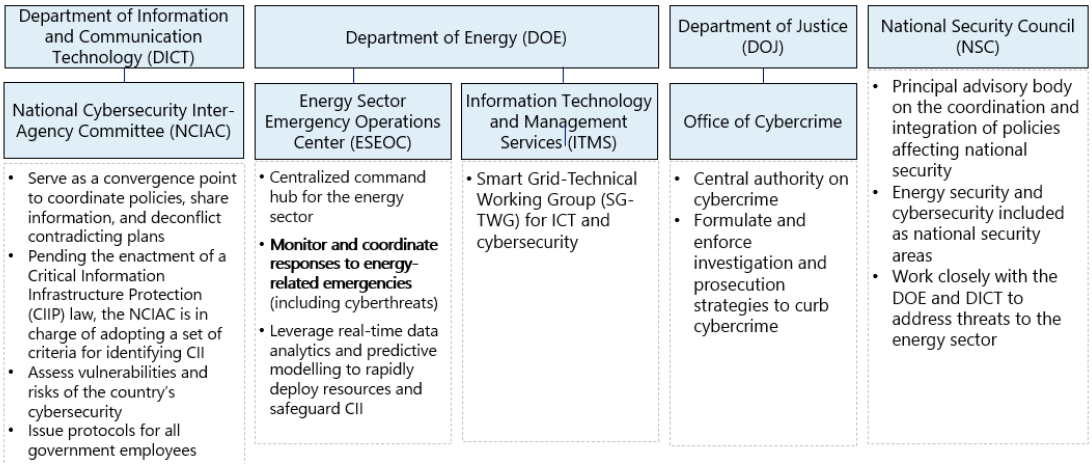
[151] GMA Integrated News (2024), DOE-GEMP latest gov't. website attacked by hackers. https://www.gmanetwork.com/news/topstories/nation/915003/doe-gemp-latest-gov-t-website-attacked-by-hackers/story/#goog_rewarded (accessed 30 July 2024).

(2) Government Structures related to Cybersecurity for DES

Cybersecurity initiatives for the energy sector are led by National Cybersecurity Inter-Agency Committee (NCIAC) which Serve as a convergence point to coordinate policies, share information, and deconflict contradicting plans[152]. DICT and DOE are the 2 key government departments in charge of formulating cybersecurity strategies for the energy sector in general. Agencies belonging to these 2 departments organise cross-department countrywide collaborative cybersecurity initiatives for the energy sector.

National Cybersecurity Inter-Agency Committee (NCIAC) and Energy Sector Emergency Operations Centre (ESEOC) play main roles to coordinate with other related departments.

Figure A.52 Overview of Government Structure related to Cyber security for DES



Source: Department of Justice[153], Government of the Philippines[154]

The NCIAC was created as a multi-disciplinary cybersecurity agency under the National Cybersecurity Plan 2023–2028 to coordinate cybersecurity efforts across the country[155]. Recognising that cybersecurity initiatives were being introduced without inter-department and inter-agency coordination, it was decided that the NCIAC should be created to harmonise efforts across the country. The NCIAC reports to the DICT, as it is the lead agency for cybersecurity policy and implementation. There is no specific mention of plans and initiatives for strengthening cybersecurity for the energy sector in this document.

[152] Government of the Philippines (2019), Designating the Philippine Statistics Authority (PSA) as the sole agency to compile and release official national accounts of the Philippines (EO No. 95, s. 2019). https://lawphil.net/executive/execord/eo2019/pdf/eo_95_2019.pdf (accessed 31 July 2024).

[153] Department of Justice (n.d.), Office of Cybercrime. https://www.doj.gov.ph/office-of-cybercrime.html (accessed 31 July 2024).

[154] Government of the Philippines (2019), Designating the Philippine Statistics Authority (PSA) as the sole agency to compile and release official national accounts of the Philippines (EO No. 95, s. 2019).

[155] Department of Information and Communications Technology, Philippines (2024), National Cybersecurity Plan 2023-2028. https://dict.gov.ph/wp-content/uploads/2024/02/NCSP-2023-2028-FINAL.pdf (accessed 31 July 2024).

(3) Policies on Cybersecurity for DES

There are government initiatives and overall guidelines for cybersecurity as a cross-industry horizontal sector. However, there are no specific initiatives or guidelines for cybersecurity in the energy sector. There are no specific cybersecurity initiatives and most of the policy only briefly touch upon the energy sector due to its classification as a sector of national security due to the presence of critical information infrastructure.

The National Cybersecurity Plan 2023–2028 mandates the Department of Information and Communications Technology (DICT) to oversee the cybersecurity strategy for the entire country[156]. This plan designates the National Cybersecurity Inter-Agency Committee (NCIAC) as the convergence point for all government agencies to share information, coordinate policies, and harmonise implementation plans. While the plan acknowledges the energy sector as one of the industries with critical infrastructure, it provides only brief mentions without delving into specific details relevant to this sector.

Similarly, the National Security Policy 2023–2028 serves as an overarching policy document that defines the strategic direction of the Philippine government in its efforts to protect, preserve, and enhance national security[157]. However, it does not offer specific guidelines or measures concerning cybersecurity for the energy sector.

Additionally, the Department Circular DC2020-02-0003 provides a national smart grid policy framework for the Philippine electric power industry and outlines a roadmap for distribution utilities (DUs)[158]. In this circular, cybersecurity is identified as a major theme within the overall smart grid development framework. It emphasises that to prevent potential cyberattacks and breaches during smart grid deployments, Generation Companies (GenCos), Transmission Network Providers (TNP), and DUs should develop a robust cybersecurity infrastructure. This infrastructure must be established in compliance with prevailing laws and regulations, as well as internationally accepted standards, although the circular does not provide further specific details.

(4) Guidelines on Cybersecurity for DES

In the National Security Policy 2023–2028 published by the National Security Council, there were mentions of energy security and cybersecurity separately. However, there were no specific strategies for cybersecurity in the energy sector. The National Security

---

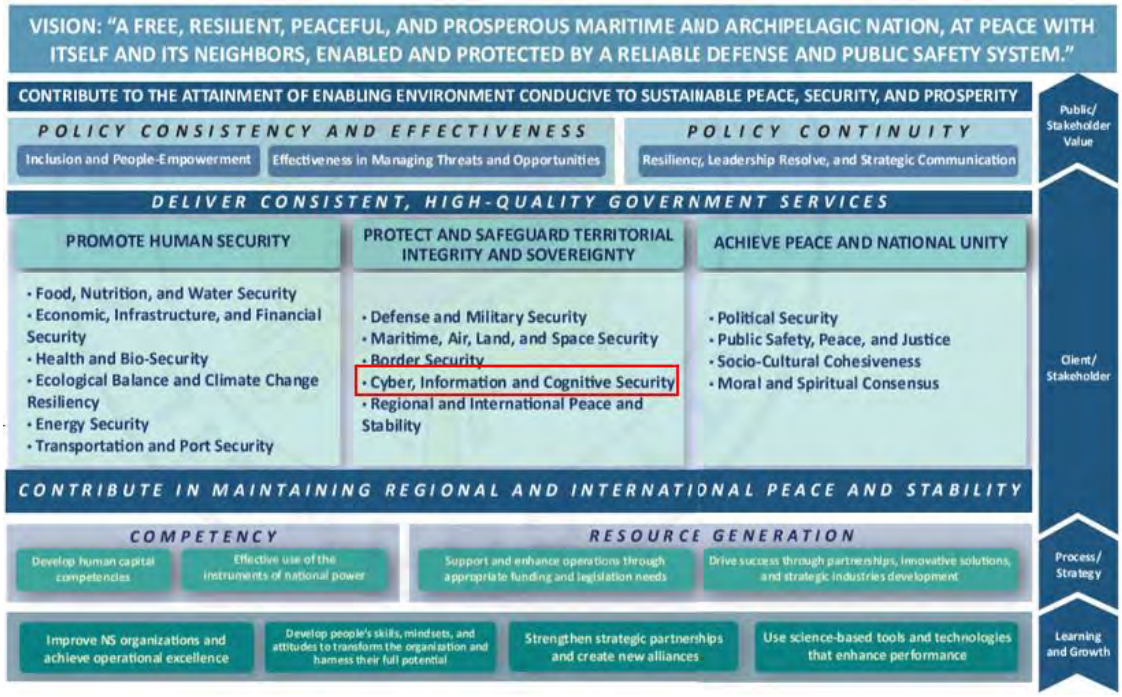
[156] Department of Information and Communications Technology, Philippines (2024), National Cybersecurity Plan 2023-2028.

[157] National Security Council, Philippines (2023), National Security Policy Manual 2023-2028. https://nsc.gov.ph/images/NSS_NSP/National_Security_Policy_Manual_FINAL_E-COPY_with_WATERMARK_140823.pdf (accessed 31 July 2024).

[158] Department of Energy, Philippines (2020), Department Circular No. DC2020-02-0003: Prescribing the policy for the Transparent and Efficient Procurement of Ancillary Services by the System Operator. https://policy.thinkbluedata.com/sites/default/files/Department%20Circular%20No.%20DC2020-02-0003.pdf (accessed 31 July 2024).

Policy 2023–2028 provides a high-level security plan for the country, though Specific cybersecurity plans for distributed energy system were not provided.

Figure A.53 National Security Policy 2023–2028



Source: National Security Council, Philippines[159]

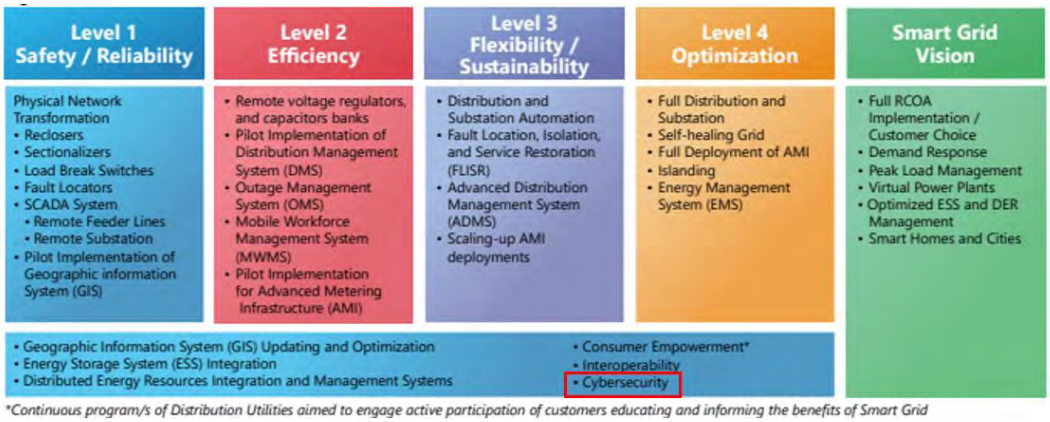
In the proposed roadmap for the energy distribution sector in the Philippine Energy Plan 2018–2040, cybersecurity is included as a programme which cuts across all 4 levels of implementation[160]. This roadmap was proposed in 2017 during a DOE-initiated Smart Grid Form and one-on-one workshops as well as focus group discussions with energy agencies, private investor-owned utilities, and electric cooperatives.

However, with reference to policies and initiatives that were introduced later, it is evident that they did not follow this proposed roadmap closely. This is perhaps due to the fact that policies and initiatives related to cybersecurity in the energy sector were released separately by different government departments and related agencies. The Philippines government tried to rectify this issue by setting up a cross-department committee known as the National Cybersecurity Inter-Agency Committee (NCIAC).

[159] National Security Council, Philippines (2023), National Security Policy Manual 2023-2028.

[160] Department of Energy, Philippines (2018), Philippine Energy Plan 2018-2040. https://policy.asiapacificenergy.org/sites/default/files/Philippine%20Energy%20Plan%202018-2040.pdf (accessed 31 July 2024).

Figure A.54 Proposed Roadmap for the Energy Distribution Sector in the Philippine Energy Plan 2018–2040



Source: Department of Energy, Philippines[161]

(5) Initiatives or Case Studies on Cybersecurity for DES

Donor countries have announced strategic partnerships with the Philippines. Most of these partnerships revolve around capacity building for the energy sector as well as developing cybersecurity capabilities.

①United States

The US government partnered with the Philippine government and private sector stakeholders to enhance cybersecurity in the energy sector. In April 2024, the Philippine Department of Energy announced the launch of the Energy Sector Emergency Operations Center (ESEOC) and the Mobile Energy System (MES) as part of USAID's $34 million Energy Secure Philippines initiative[162].

To enhance resilient energy infrastructure and emergency response capabilities, the Department of Energy inaugurated the ESEOC and the Mobile Energy System (MES). The ESEOC acts as a centralised command centre that utilises technologies from Europe and the United States to oversee, evaluate, and coordinate responses to various energy-related emergencies. The Mobile Energy Systems complement the ESEOC with a fleet of versatile, scalable solutions designed for rapid deployment during emergencies. These modular systems incorporate renewable energy sources, energy storage, and microgrid technologies to provide reliable power generation and distribution in remote or disaster-affected areas.

[161] Department of Energy, Philippines (2018), Philippine Energy Plan 2018-2040.

[162] Power Philippines (2021), USAID sets aside Php1.6B for clean energy projects. https://powerphilippines.com/usaid-sets-aside-php1-6b-for-clean-energy-projects/ (accessed 2 August 2024).

②Japan

In July 2024, JICA held a 3-day Cybersecurity Risk Management workshop for an ongoing project with the DICT for the capacity development on cybersecurity.

Participants from various Philippine government department and agencies including the DOE attended the workshop[163].

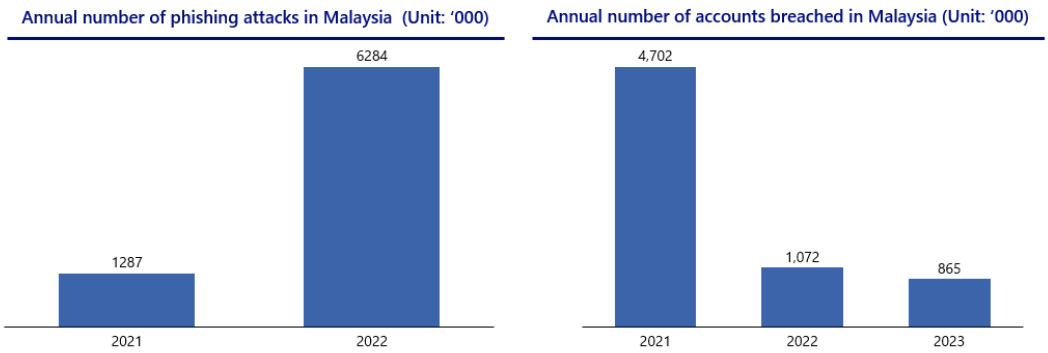
③Australia

In 2023, the Australian and Philippine governments jointly declared a Strategic Partnership. This partnership includes an agreement to cooperate on defence and cybersecurity as well as support the clean energy transition[164].

1-2-3. Malaysia

(1) Overview on Cybersecurity

Figure A.55 Overview of Cybersecurity in Malaysia



Source: Malaysia Computer Emergency Response Team (MyCERT)[165], Tech2Thai[166]

[163] Japan International Cooperation Agency (JICA) (2024), JICA backs PH government's efforts in safeguarding cyberspace. https://www.jica.go.jp/english/overseas/philippine/information/press/2024/1545307_53492.html (accessed 2 August 2024).

[164] Prime Minister of Australia (2023), Joint Declaration on a Strategic Partnership between the Republic of the Philippines and the Commonwealth of Australia. https://www.pm.gov.au/media/joint-declaration-strategic-partnership-between-republic-philippines-and-commonwealth (accessed 2 August 2024).

[165] Malaysia Computer Emergency Response Team (MyCERT) (2023), Incident Statistics 2023. https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=2862eb40-2bc0-4b4e-90ed-07d4eef73b7b (accessed 3 August 2024).

[166] Tech2Thai (n.d), Six months of phishing attacks in 2022 exceed SEA's total number last year. https://www.tech2thai.com/enterprise_tech/1990/six-months-of-phishing-attacks-in-2022-exceed-sea-rsquo-s-total-number-last-year

There is a significant surge in phishing attacks in Malaysia, with the number of incidents rising from 1.28 million in 2021 to 6.28 million in 2022 – a nearly fivefold increase. This sharp escalation points to a dramatic rise in cybercriminal activities, or alternatively, could reflect enhanced detection and reporting mechanisms. As phishing remains one of the primary attack vectors in cybersecurity, this spike is alarming and suggests that Malaysia's threat landscape has become increasingly hostile over a short period.

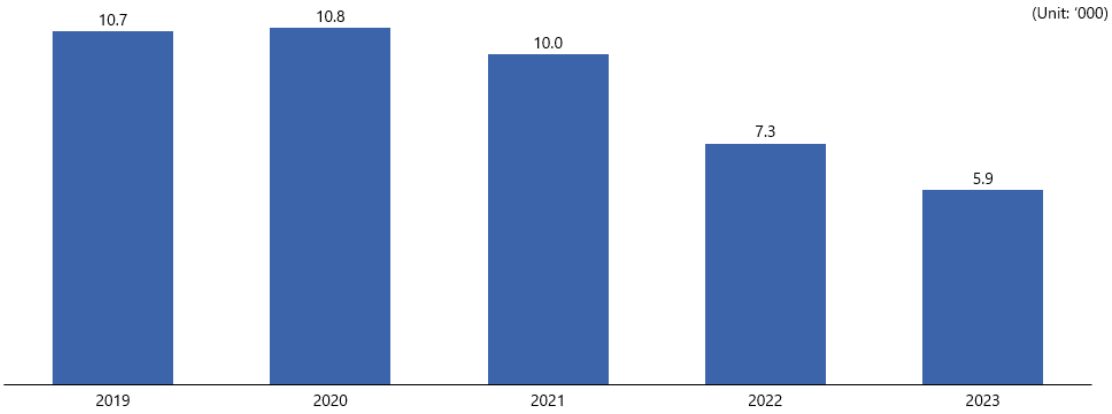
In parallel, Malaysia's cybersecurity challenges are further underscored by recent breach statistics. According to Surfshark's Q3 2023 report, Malaysia was the eighth most breached country, with a 144% increase in breach rates compared to the previous quarter (Q2 2023). This leap indicates that while phishing attacks surged in 2022, data breaches continued to be a pressing issue into 2023[167]. Additionally, Malaysia ranked fifth in breach density, suggesting that a higher-than-average portion of its population is affected by cyber breaches. However, a downward trend in breaches over three years was observed, with the total number of breached accounts significantly decreasing from the first to the second year and continuing to decline, albeit more slowly, in the third year. This reduction might suggest that Malaysia is making progress in improving cybersecurity defences or that attackers are shifting to different tactics, such as phishing.

Furthermore, Fortinet's 2022 report paints a concerning picture of cyber intrusions in Malaysia's Operational Technology (OT) sector, with 100% of OT companies experiencing at least one cyber intrusion in the past year. Not only did these intrusions disrupt operations, but 59% of Malaysian businesses reported productivity-impacting outages. More alarmingly, 90% of these intrusions took hours or longer to restore service, highlighting the significant operational costs and downtime associated with such attacks.

This combination of phishing escalation, frequent breaches, and OT sector vulnerabilities presents a multifaceted cybersecurity challenge for Malaysia. While some sectors have shown signs of improvement, as seen in the breach rate decline over three years, the persistence of operational outages and the magnitude of phishing attacks indicate that Malaysia still faces critical risks to its cybersecurity infrastructure. This necessitates not only robust technological defences but also widespread organisational preparedness and response strategies to mitigate the growing threat landscape.

[167] The Star (2023), Cybersecurity report ranks Malaysia as eighth most breached country in Q3 2023. https://www.thestar.com.my/tech/tech-news/2023/12/06/cybersecurity-report-ranks-malaysia-as-eighth-most-breached-country-in-q3-2023

Figure A.56 Number of Reported Incidents Dealt by MyCERT in Malaysia



Source: Malaysia Computer Emergency Response Team (MyCERT)[168]

The data on reported cybersecurity incidents in Malaysia from 2019 to 2023 reveals a relatively stable landscape in the earlier years, followed by a significant decline. Between 2019 and 2020, the number of incidents remained stable, increasing only marginally from 10.7 thousand to 10.8 thousand. This slight uptick likely reflects growing cyber activity, with phishing emails, malware, and insider breaches identified as the top three types of intrusions that businesses in Malaysia experienced during this period.

However, starting from 2021, there was a notable decrease in reported incidents, dropping from 10 thousand in 2021 to 7 thousand in 2022 and further declining to 5.9 thousand in 2023. This downward trend suggests that Malaysia has made tangible progress in its cybersecurity efforts. The reduced number of incidents could indicate the successful implementation of preventive and defensive measures, such as enhanced cybersecurity policies, increased awareness and training programmes, and improved incident response capabilities.

Despite the overall decrease in incidents, the data shows that the threat landscape in Malaysia remains dynamic, with some types of attacks, like phishing, surging in recent years. The stabilisation followed by a decline in reported incidents implies that while significant progress has been made, continuous adaptation is necessary to keep pace with evolving cyber threats. This also highlights the importance of further investments in both technology and human capital to maintain and strengthen cybersecurity defences across sectors.

[168] Malaysia Computer Emergency Response Team (MyCERT) (2023), Incident Statistics 2023.

Figure A.57 Notable Cases of Cyberattacks on DES in Malaysia

Country	Type of attack	Year	Incident	Overview	Impact
Malaysia	Data Breach	2024	The international hacker group R00TK1T claimed to have attacked Malaysia's entire **EV charging infrastructure**	R00TK1T breached the GO TO-U (GTU) EV charging platform that TNB Electron's subsidiary, TNBX uses.	• Go To-U said that it did not find any evidence of security breaches on its systems, despite the claims made by R00TK1T. According to TNBX's website, • there were 3 active TNB Electron DC fast chargers throughout Peninsular Malaysia, and 13 TNBX DC fast charging points at various automobile showrooms.
Malaysia	Ransomware	2024	The ransomware group Rhysida cyberattacked Malaysian Industrial Development Finance Bnd (MIDF)	Rhysida posted on social media platforms to urge potential buyers to "seize the opportunity to acquire exclusive and sensitive data" from the institution within 7 days.	• MIDF subsequently reported the cyberattack to relevant authorities. • MIDF is a financial institution pivotal to the modernization of Malaysia's manufacturing industries

Source: The Cyber Express[169], SoyaCincau[170]

In 2024, the hacker group R00TK1T claimed to have breached Malaysia's electric vehicle (EV) charging infrastructure. However, subsequent investigations found no evidence supporting the breach. Additionally, the ransomware group Rhysida targeted the Malaysian Industrial Development Finance Bhd (MIDF). They threatened to sell stolen data, which led MIDF to report the incident to the authorities.

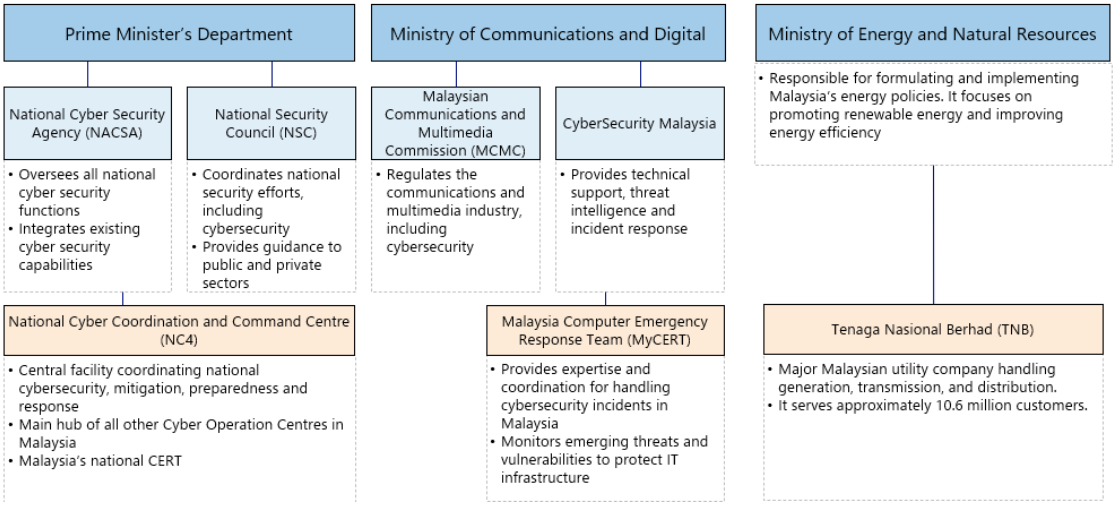
(2) Government Structures related to Cybersecurity for DES

In Malaysia, cybersecurity governance is coordinated by several key government agencies and industry players, with oversight from the Prime Minister's Department, the Ministry of Communications and Digital and Ministry of Energy and Natural Resources. These bodies are responsible for driving national cybersecurity policies and ensuring the integration of capabilities across public and private sectors.

[169] The Cyber Express (2024), MIDF cyberattack claims by Rhysida. https://thecyberexpress.com/midf-cyberattack-claims-by-rhysida/ (accessed 3 August 2024).

[170] SoyaCincau (2024), Go To-U claims R00tk1t compromised TNB Electron app, affecting TNBX. https://soyacincau.com/2024/02/19/go-to-u-claims-r00tk1t-tnb-electron-tnbx/ (accessed 4 September 2024).

Figure A.58 Overview of Related Organisations



Source: National Security Council, Malaysia[171]

Under the Prime Minister's Department, the National Cyber Security Agency (NACSA) is responsible for overseeing all national cybersecurity functions and integrating existing capabilities. The National Security Council (NSC) coordinates national security efforts, including cybersecurity, and provides guidance to both the public and private sectors.

Within NACSA, the National Cyber Coordination and Command Centre (NC4) serves as the central facility for coordinating Malaysia's cybersecurity efforts. It acts as the main hub, overseeing mitigation, preparedness, and response activities, and connects with other cyber operation centres across the country.

Under the Ministry of Communications and Digital, the Malaysian Communications and Multimedia Commission (MCMC) regulates the communications and multimedia industry, including overseeing cybersecurity measures. Additionally, CyberSecurity Malaysia provides technical support, threat intelligence, and incident response services. Within CyberSecurity Malaysia, the Malaysia Computer Emergency Response Team (MyCERT) is the primary body responsible for handling and coordinating cybersecurity incidents, offering specialised expertise in managing cyber threats.

The Ministry of Energy and Natural Resources is tasked with formulating and implementing Malaysia's energy policies, with a focus on promoting renewable energy and improving energy efficiency. A key entity under this ministry is Tenaga Nasional Berhad (TNB), Malaysia's largest utility company, responsible for the generation, transmission, and distribution of energy[172]. TNB plays a critical role in securing the nation's energy infrastructure, especially through its smart grid and operational

[171] National Security Council, Malaysia (2020), Malaysia Cyber Security Strategy 2020-2024. https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf (accessed 4 September 2024).

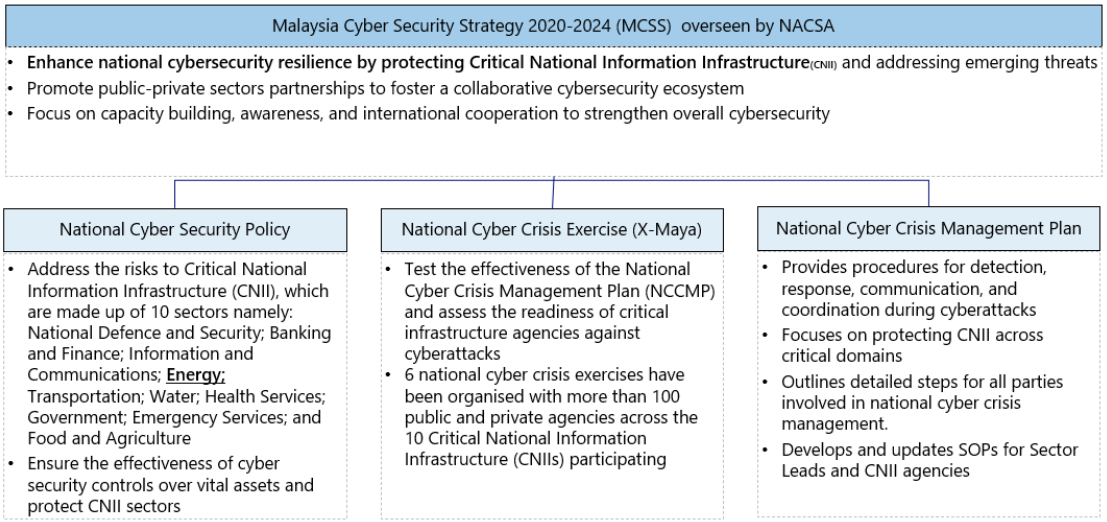
[172] Tenaga Nasional Berhad (TNB) (n.d), About TNB. https://www.tnb.com.my/about-tnb (accessed 4 September 2024).

technology cybersecurity initiatives.

(3) Policies on Cybersecurity for DES

Malaysia has adopted a cautious and strategic approach to cybersecurity through its Cyber Security Strategy 2020–2024 (MCSS), which is overseen by the National Cyber Security Agency (NACSA)[173]. This strategy focuses on protecting critical infrastructure, fostering public–private collaboration, and enhancing national resilience against emerging cyber threats.

Figure A.590verview of Policies



Source: CyberSecurity Malaysia[174]

1. National Cyber Security Policy

A core objective of MCSS is to safeguard Critical National Information Infrastructure (CNII), which encompasses 10 key sectors: National Defence and Security, Banking and Finance, Information and Communications, Energy, Transportation, Water, Health Services, Government, Emergency Services, and Food and Agriculture. This ensures the effectiveness of cybersecurity controls over these vital sectors to protect their operations from cyberattacks.

2. National Cyber Crisis Exercises (X-Maya)

Malaysia conducts National Cyber Crisis Exercises (X-Maya) to test and improve its cyber

[173] CyberSecurity Malaysia (2020), CyberSecurity Malaysia Annual Report 2020. https://www.cybersecurity.my/data/content_files/46/2464.pdf (accessed 4 September 2024).

[174] CyberSecurity Malaysia (2020), CyberSecurity Malaysia Annual Report 2020.

crisis management readiness. These exercises, which are part of the National Cyber Crisis Management Plan (NCCMP), involve over 100 public and private agencies across the 10 CNII sectors. So far, six national cyber crisis exercises have been held, designed to assess the readiness of critical infrastructure agencies to withstand cyberattacks[175].

3. National Cyber Crisis Management Plan (NCCMP)

The NCCMP provides a framework for detection, response, communication, and coordination during cyber incidents. Its primary focus is on protecting CNII and ensuring that all parties involved, including Sector Leads and CNII agencies, follow detailed standard operating procedures (SOPs).

The NCCMP is regularly updated to reflect evolving cyber threats, with the goal of ensuring the continuous improvement of crisis management protocols[176].

Through these initiatives, Malaysia is reinforcing its cybersecurity capabilities, improving its preparedness for national cyber crises, and ensuring that both public and private sectors are aligned in addressing emerging threats to critical infrastructure.

(4) Guidelines on Cybersecurity for DES

Tenaga Nasional Berhad (TNB) emphasises a structured and evolving approach to cybersecurity, utilising well-established frameworks to address sophisticated threats. The company advocates the use of frameworks such as NIST Cybersecurity Framework (NIST-CSF), ISO/IEC 27001, and IEC 62443, highlighting the importance of continuously adapting strategies and upgrading physical security measures to stay ahead of emerging risks.

Table A.15 Overview of Cybersecurity Measures

Key Cybersecurity Practices at TNB	Description
1. ISO/IEC 27001:2013 Certification	TNB has achieved and annually renews its ISO/IEC 27001:2013 certification, covering its power generation, transmission, distribution, and digital systems. This certification includes critical infrastructure components such as Distributed Control Systems (DCS) and SCADA systems. The most recent renewal was completed on November 10, 2023, ensuring ongoing compliance with international information security management standards.
2. Smart Meter Security	TNB secures its smart meters and Advanced Metering Infrastructure (AMI) systems by employing the Device Language Message Specification/Companion Specification for Energy Metering (DLMS/COSEM) protocol. This approach is based on NIST standards, which helps protect against unauthorised access and data breaches.

[175] National Security Council, Malaysia (2020), Malaysia Cyber Security Strategy 2020-2024.

[176] National Cyber Security Agency (NACSA) (n.d), National Cyber Crisis Management Plan (NCCMP). https://www.nacsa.gov.my/nccmp.php (accessed 4 September 2024).

3. Advanced Distributed Management System (ADMS) Compliance	TNB adheres to OT cybersecurity standards such as IEC 62351 and NIST recommendations for system hardening and security best practices. This compliance ensures that their Advanced Distributed Management System (ADMS) is resilient to cyber threats and capable of maintaining operational integrity.
4. Recognition and Awards	TNB's robust cybersecurity measures have earned recognition, including the 'Cyber Security Project of the Year 2019' award. Additionally, TNB is included in the Share Guide Association Malaysia (SGAM) IT Users Group, reflecting its standing in the industry for effective cybersecurity practices.

Source: Tenaga Nasional Berhad[177]

(5) Initiatives or Case Studies on Cybersecurity for DES

Malaysia has actively engaged in regional cybersecurity and digital integration efforts, collaborating with international and regional partners to enhance its cybersecurity posture and support broader ASEAN initiatives. Key contributions and partnerships with the United States, Japan, Australia, and the Asian Development Bank (ADB) highlight Malaysia's commitment to strengthening its digital infrastructure and cybersecurity resilience.

Figure A.60 Supporting Initiatives from Foreign Countries

United States	• USAID aids ASEAN in **boosting regional internet connectivity and accessibility by promoting strategies that reinforce cybersecurity**, digital finance, and governance. • USAID also assisted ASEAN in creating **its Digital Integration Framework and developing the ASEAN Digital Integration Index** which is a tool for tracking progress in its implementation.
Japan	• In Feb 2024, the National Cyber Security Agency **(NCSA)** of Thailand and the National Center of Incident Readiness and Strategy for Cybersecurity **(NISC)** of Japan co-hosted the **ASEAN-Japan cybersecurity Working Group Meeting** to promote effective problem-solving, maintain stability and cybersecurity of Government Agencies and Critical Information Infrastructure Organizations, and develop capabilities and skills in responding to cyber threats. • The ASEAN-Japan Cybersecurity Working Group Meeting in February 2024, co-hosted by Thailand's NCSA and Japan's NISC, was an ASEAN-wide event aimed at promoting cybersecurity across the region, including Malaysia.
Australia	• Australia's International Cyber and Critical Technology Engagement Strategy, launched in 2021, emphasizes regional cooperation with ASEAN, which supports cyber capacity building in ASEAN countries.
ADB	• ADB has proposed a technical assistance (TA) project to enhance DMCs' cybersecurity resilience by incorporating cybersecurity measures within ADB's lending operations • The TA aims to strengthen regional knowledge on implementing cybersecurity measures, enhance the capacity of selected DMCs, and support the implementation of projects incorporating cybersecurity measures

Source: Asian Development Bank (ADB)[178], 360info[179]

[177] Tenaga Nasional Berhad (TNB) (n.d), Smart Grid. https://www.tnb.com.my/smart-grid/ (accessed 4 September 2024).

[178] Asian Development Bank (ADB) (2024), Southeast Asia Energy Transition Partnership (formerly Southeast Asia Green Recovery Program). https://www.adb.org/projects/58029-001/main (accessed 5 September 2024).

[179] 360info (2024), Southeast Asia's three-nation partnership to fight cyber threats. https://360info.org/southeast-asias-three-nation-partnership-to-fight-cyber-threats/ (accessed 5 September 2024).

USAID has been instrumental in supporting Malaysia and ASEAN with digital integration and cybersecurity efforts. Key initiatives include:

- Digital Integration Framework: USAID's assistance in creating the ASEAN Digital Integration Framework has facilitated Malaysia's participation in a regional approach to digital transformation.
- ASEAN Digital Integration Index: This tool, developed with USAID support, helps Malaysia track and measure progress in implementing digital integration strategies, contributing to improved regional connectivity and cybersecurity.

In February 2024, Malaysia was involved in the ASEAN–Japan Cybersecurity Working Group Meeting co-hosted by Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and Thailand's National Cyber Security Agency (NCSA). Key outcomes relevant to Malaysia include:

- Regional Cybersecurity Promotion: The meeting emphasised Malaysia's role in enhancing regional cybersecurity through collaborative efforts and knowledge sharing.
- Stability and Cybersecurity: Discussions focused on maintaining stability and protecting critical infrastructure, aligning with Malaysia's own cybersecurity objectives and strategies.
- Capability Development: Malaysia's participation in this event contributed to building regional capabilities in addressing and managing cyber threats effectively.

Australia's International Cyber and Critical Technology Engagement Strategy has supported Malaysia's cybersecurity and digital integration efforts[180]. Notable aspects include:

- Cyber Capacity Building: Australia's strategy has provided resources and support to enhance Malaysia's cybersecurity capabilities, contributing to a more secure digital environment.
- Regional Cooperation: Through this strategy, Malaysia has benefited from regional cooperation initiatives that promote shared cybersecurity practices and frameworks.

The ADB has proposed a technical assistance (TA) project designed to bolster cybersecurity resilience amongst its developing member countries, including Malaysia[181]. Key components of this initiative include:

- Cybersecurity Integration: The TA project aims to incorporate cybersecurity measures into ADB's lending operations, which benefits Malaysia by ensuring that

[180] 360info (2024), Southeast Asia's three-nation partnership to fight cyber threats.

[181] Asian Development Bank (ADB) (2024), Southeast Asia Energy Transition Partnership (formerly Southeast Asia Green Recovery Program).

funded projects adhere to high cybersecurity standards.

- Knowledge and Capacity Building: The project focuses on enhancing Malaysia's knowledge and capacity in implementing effective cybersecurity measures.
- Support for Implementation: By supporting the implementation of cybersecurity measures in various projects, the TA project strengthens Malaysia's overall cybersecurity framework.

The inaugural NACSA Cyber Security Summit (NCSS) 2024 took place from July 30 to August 1, 2024, at the Putrajaya International Convention Centre. Organised by the National Cyber Security Agency (NACSA) in collaboration with Alpine Integrated Solution Sdn Bhd, the summit served as a premier platform for cybersecurity professionals and industry leaders.

Additionally, on 2024, Group-IB, a leading cybersecurity firm founded in 2003 and headquartered in Singapore, and CyberSecurity Malaysia, the national cybersecurity agency, formalised their collaboration with the signing of a Memorandum of Understanding (MOU) in Kuala Lumpur[182]. This strategic partnership is designed to enhance Malaysia's cyber resilience and protect critical IT infrastructure through several key initiatives.

BlackBerry, EY, Thales, Google Cloud Security, Fortinet, Microsoft, Siemens Energy, Tenable, and Huawei are sponsoring various sessions at the NACSA Cyber Security Summit (NCSS) 2024. These companies are expected to offer cybersecurity solutions and expertise to bolster Malaysia's cybersecurity initiatives.

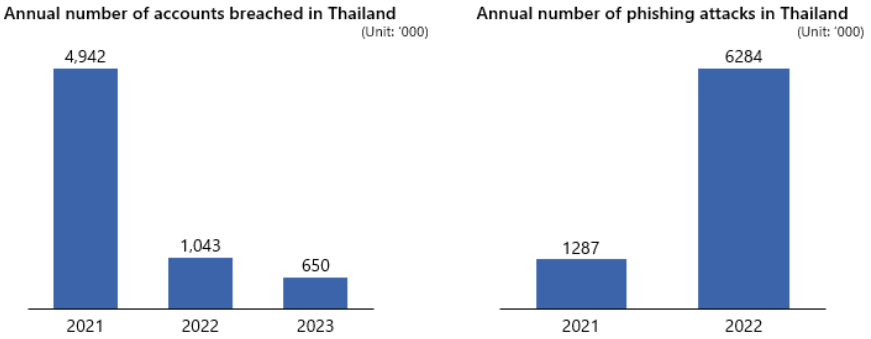
1-2-4. Thailand

(1) Overview on Cybersecurity

Thailand has experienced a range of cyberattacks, including ransomware, phishing, remote desktop attacks, and other forms of data exfiltration. Despite these challenges, local efforts, particularly the enactment of the Cybersecurity Act in 2019, have led to increased cybersecurity awareness amongst organisations. This heightened awareness may be contributing to the observed decline in the number of accounts breached over recent years.

[182] Bastille Post (2024), Defending Malaysia's cybersecurity: Group-IB and CyberSecurity Malaysia forge strategic alliance to safeguard national cyber resilience. https://www.bastillepost.com/global/article/4057698-defending-malaysias-cybersecurity-group-ib-and-cybersecurity-malaysia-forge-strategic-alliance-to-safeguard-national-cyber-resilience (accessed 5 September 2024).

Figure A.61 Overview of Cybersecurity in Thailand



Source: Bangkok Post[183]

This decline suggests that cybersecurity measures and awareness are having a positive impact. However, the trend of digitalisation continues to drive an increase in phishing attempts, highlighting an ongoing challenge. Despite improvements in overall breach numbers, the rise in phishing attempts underscores the need for continued vigilance and robust cybersecurity practices to address evolving threats in Thailand's digital landscape.

Figure A.62 Notable Cases of Cyberattacks on DES in Thailand

Country	Type of attack	Year	Incident	Overview	Impact
Thailand	Phishing	2023	• There were fake SMS links claiming to be government agencies and financial institutions to deceive money	• Upon clicking the link, a remote-control application was installed and money was transferred from the victim's bank account via Mobile Banking	• The Cyber Crime Investigation Bureau arrested 6 perpetrators, 5 communication antenna counterfeiting devices and 4 cars
Thailand	Data Breach	2022	• An Initial Access Broker (IAB) was found selling access to nuclear research organisations	• The IAB had gain access to compromised employees' Office 365 accounts, and was monetising the stolen INER credentials through a trusted network of contacts in the dark web	• The nuclear research organizations in Thailand, Taiwan, Vietnam, Brunei, and Malaysia all had their data stolen and monetized.

Source: Resecurity[184], National Cyber Security Agency (NCSA)[185]

---

[183] Bangkok Post (2024), Thailand tops region for ransomware attacks. https://www.bangkokpost.com/business/general/2792735/thailand-tops-region-for-ransomware-attacks (accessed 5 September 2024).

[184] Resecurity (2023), Ransomware Attacks against the Energy Sector on the rise - Nuclear and Oil & Gas are Major Targets in 2024. https://www.resecurity.com/blog/article/ransomware-attacks-against-the-energy-sector-on-the-rise-nuclear-and-oil-gas-are-major-targets-2024 (accessed 5 September 2024).

[185] National Cyber Security Agency (NCSA) (2023), Annual Report 2023 (**รายงานประจำปี สกมช.** 2566). https://ncsa.or.th/Ebook_%E0%B8%A3%E0%B8%B2%E0%B8%A2%E0%B8%87%E0%B8%B2%E0%B8%99%20%E0%B8%AA%E0%B8%81%E0%B8%A1%E0%B8%8A/%E0%B8%A3%E0%B8%B2%E0%B8%A2%E0%B8%87%E0%B8%B2%E0%B8%99%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%88%E0%B8%B3%E0%B8%9B%E0%B8%B5%20%E0%B8%AA%E0%B8%81%E0%B8%A1%E0%B8%8A%202566.html? (accessed 5 September 2024).

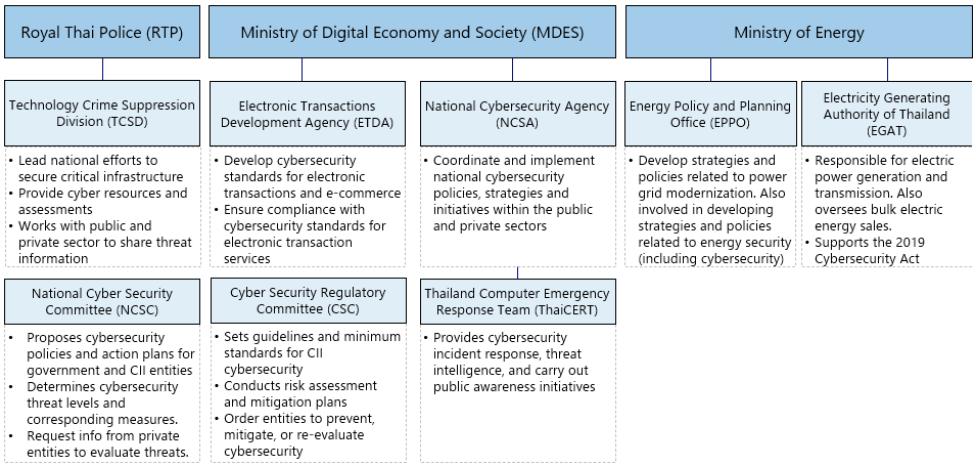
While there are no specific examples of cyberattacks on the energy sector in Thailand publicly documented, there have been notable cyber incidents that highlight broader security concerns. For instance, in 2023, a cyberattack involved fake SMS links that impersonated government agencies and financial institutions to deceive victims. Clicking these links installed a remote-control application on the victims' devices, leading to unauthorised transfers of money from their bank accounts via mobile banking. The Cyber Crime Investigation Bureau responded by arresting six perpetrators and seizing five communication antenna counterfeiting devices and four cars.

Additionally, in 2022, an Initial Access Broker (IAB) was discovered selling access to nuclear research organisations. This broker had compromised employees' Office 365 accounts and was monetising stolen credentials, including those from the International Nuclear Energy Research (INER), through a network of contacts on the dark web. These incidents underscore the evolving nature of cyber threats and the importance of robust cybersecurity measures to protect sensitive information and critical infrastructure.

(2) Government Structures related to Cybersecurity for DES

In Thailand, several government ministries and federal agencies are spearheading various cybersecurity initiatives, which are relevant to cybersecurity of distributed energy systems. Notably, the Energy Policy and Planning Office (EPPO) under the Ministry of Energy plays a key role. The EPPO is responsible for developing strategies and policies related to power grid modernisation and energy security, including cybersecurity.

Figure A.63 Overview of Relevant Organisations



Source: Thai Computer Emergency Response Team[186], Asia Law Portal[187]

[186] Thai Computer Emergency Response Team (ThaiCERT) (n.d), About NCERT. https://www.thaicert.or.th/en/about-ncert/ (accessed 5 September 2024).

[187] Cybersecurity Law: Thailand (2019), Cybersecurity Law: Thailand. https://asialawportal.com/cybersecurity-law-in-thailand/ (accessed 5 September 2024).

One significant initiative is the EPPO's Project for the Development of Cybersecurity Systems (EPPO-02). This project is part of the broader Master Plan for Smart Grid Network System Development. It aligns with the objectives of the Cybersecurity Act (2019) and integrates its goals into the project's framework. The EPPO-02 project focuses on enhancing cybersecurity measures within Thailand's energy sector, ensuring that the power grid and related infrastructures are protected against evolving cyber threats. Through these initiatives, Thailand aims to strengthen its cybersecurity posture in alignment with national regulations and international best practices.

(3) Policies on Cybersecurity for DES

The EPPO has initiated the Project for Development of Cybersecurity Systems to support Thailand's future smart grid infrastructure. This project is part of the broader Master Plan for Smart Grid Network System Development (2015–2036), which was introduced by the Ministry of Energy[188]. The primary objective of the EPPO's project is to establish a comprehensive cybersecurity development plan tailored to the smart grid, ensuring that the grid's digital infrastructure is resilient against cyber threats. This initiative reflects a commitment to integrating robust cybersecurity measures into the nation's energy sector, aligning with the strategic goals outlined in the Master Plan.

During Stage 2, the Energy Policy and Planning Office (EPPO) identified eight key tasks aimed at developing a cybersecurity plan aligned with the country's Smart Grid Plan. The plan set forth a roadmap for implementing cybersecurity measures starting from Stage 3, with the ultimate goal of achieving 'pervasive cybersecurity' by Stage 4.

Despite the EPPO's announcement in 2019 of awarding projects to specific consulting companies for cybersecurity implementation, there have been no further updates on the progress of these initiatives. Additionally, as of 2023, no specific budget has been allocated for cybersecurity under the smart grid programme. Funding has been directed towards broader energy security measures instead. This lack of dedicated funding highlights a gap in the ongoing development and enhancement of cybersecurity infrastructure within Thailand's smart grid framework.

In 2015, the Ministry of Energy of Thailand launched the Master Plan for Smart Grid Network System Development in Thailand 2015–2036

This Master Plan is divided into 4 phases

- 2015–2016: Preparation Phase
- 2017–2021: Short-Term Phase

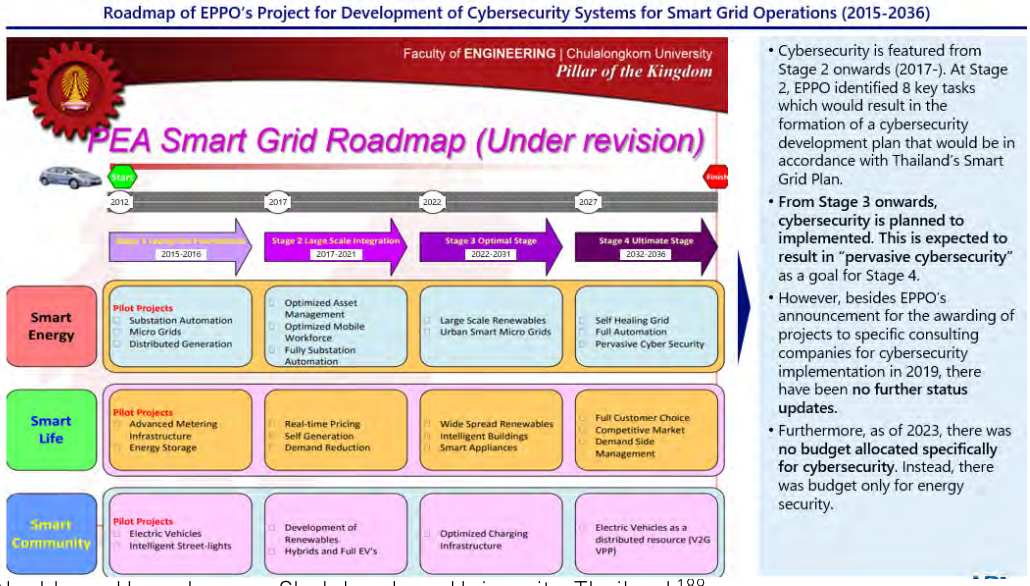
[188] Ministry of Energy (2015), THAILAND: Master Plan for Smart Grid Network System Development in Thailand 2015-2036. https://policy.asiapacificenergy.org/node/4348 (accessed 5 September 2024).

- 2022–2031: Medium-Term Phase
- 2032–2036: Long-Term Phase

For the Short-Term Phase of 2017–2021, the Energy Policy and Planning Office (EPPO) identified several key tasks, one of which was ensuring the cybersecurity of the smart grid network system. The overall scope of this Project is as follows:

- Study and review information on cyber threats in the electrical system
- Study relevant guidelines, policies, laws, standards, and regulations in foreign electrical systems
- Understand current trends in ICT and its relevance to Thailand's smart grid operations
- Assess risk level of cyber threats to Thailand's electrical system (present and future)
- Set the scope and guidelines for smart grid cybersecurity
- Analyse policies, laws, regulations and make suggestions
- Recommend management structures for short- to long-term
- Create an overall cybersecurity development plan in accordance with Thailand's Smart Grid Master Plan

Figure A.64 Roadmap of EPPO's Project



Source: Naebboon Hoonchareon, Chulalongkorn University, Thailand.[189]

[189] Naebboon Hoonchareon, Chulalongkorn University, TH. (2015), Thailand Smart Grid Policy Plan and Roadmaps.

(4) Guidelines on Cybersecurity for DES

In Thailand, several government cybersecurity guidelines are crucial for regulating the energy sector. The primary regulation is the Cybersecurity Act, which provides the legal framework for cybersecurity operations, sets key obligations for critical information infrastructure (CII) organisations, and promotes public–private cooperation[190]. The Act also outlines penalties for non-compliance, ensuring adherence to cybersecurity standards.

Complementing the Cybersecurity Act, the Cloud Cybersecurity Standards address risks associated with cloud services utilised by government agencies, regulatory organisations, and CII entities. These standards focus on cloud security governance and the protection of cloud infrastructure and operations. Organisations using cloud services must evaluate their technology information systems' impact levels and adopt relevant standards to mitigate cyber threats effectively.

Additionally, the Notification on Baseline Cybersecurity Standards mandates that CII organisations, including those in the energy sector, conduct self-assessments and categorise their data and IT systems into one of three risk classes. Based on their risk classification, these organisations are required to implement baseline cybersecurity measures tailored to their specific needs and vulnerabilities. These guidelines collectively ensure a robust cybersecurity posture for critical infrastructure within Thailand.

(5) Initiatives or Case Studies on Cybersecurity for DES

In 2023, the National Cyber Security Agency (NCSA) organised the Cyber Clinic initiative to enhance cybersecurity capabilities across Thailand. This programme featured a series of workshops specifically designed for government agencies, regulators, and critical information infrastructure (CII) entities. A total of 10 seminars were conducted, attracting approximately 1,600 participants from 74 government agencies, regulatory bodies, CIIs, and 17 private organisations. The goal was to improve the skills of cybersecurity officers and raise cybersecurity awareness amongst target agencies[191].

In addition, the Cybersecurity Research Lab at the National Electronics and Computer Technology Centre (NECTEC) plays a pivotal role in advancing cybersecurity research and development[192]. NECTEC focuses on responding to the needs of seven industrial target

---

https://policy.asiapacificenergy.org/sites/default/files/Master%20Plan%20for%20Smart%20Grid%20Network%20System%20Development%20in%20Thailand%202015-2036%20%28Presentation%29%20%28EN%29.pdf (accessed 5 September 2024).

[190] Professor Pawee Jenweeranon (n.d), Thailand's Cyber Resilience Journey: Understanding Obstacles and Uncovering Remedies. https://techforgoodinstitute.org/blog/expert-opinion/thailands-cyber-resilience-journey-understanding-obstacles-and-uncovering-remedies/

[191] Asia Law Portal (2019), Cybersecurity Law: Thailand.

[192] National Electronics and Computer Technology Center (NECTEC) (n.d), Research. https://www.nectec.or.th/en/research

groups, including National Security and Cybersecurity, aligning its efforts with the National Economic and Social Development Plan. This lab supports the development of innovative solutions and strategies to address emerging cybersecurity challenges and enhance national security.

While there are examples of cross-border collaboration between Thailand and donor countries on cybersecurity, there are currently no specific case studies addressing cybersecurity for Distributed Energy Systems (DES).

Thailand's efforts to bolster cybersecurity include significant international support, particularly from the USAID and Japan. USAID supports ASEAN in enhancing regional internet connectivity and accessibility through strategies that strengthen cybersecurity, digital finance, and governance[193].

Japan has also played a vital role in Thailand's cybersecurity landscape. In February 2024, Thailand's National Cyber Security Agency (NCSA) and Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) co-hosted the ASEAN–Japan Cybersecurity Working Group Meeting. This meeting aimed to foster effective problem-solving, maintain stability, and enhance cybersecurity capabilities for government agencies and Critical Information Infrastructure (CII) organisations, focusing on skill development and cyber threat response.

Additionally, in 2018, Thailand and Japan collaborated to establish the ASEAN–Japan Cybersecurity Capacity Building Centre (AJCCBC). This centre focuses on improving the expertise of government personnel and CII organisations in managing, preventing, and responding to cyber threats, further strengthening regional cybersecurity efforts[194].

1-2-5. Indonesia

(1) Overview on Cybersecurity

The National Cybersecurity and Cryptography Agency of Indonesia has identified AP40 as a significant advanced persistent threat (APT) targeting the energy industry. Basically, Advanced Persistent Threat (APT) is a cyberthreat actor that is usually state-sponsored or other large organisation with the aim of gaining unauthorised access to computer network and remain undetected for a long period of time. One of the major APT is APT40. APT40 is known for its sophisticated tactics focusing on intelligence gathering, espionage, and data theft. These activities pose a serious risk to national security by compromising critical infrastructure, including power generation facilities, shipping lines, and ocean-

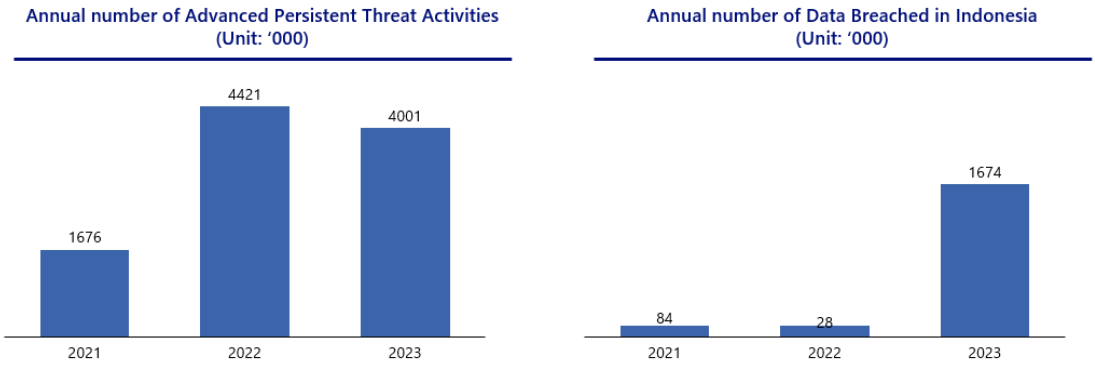
[193] U.S. Mission to ASEAN (n.d), USAID ASEAN. https://asean.usmission.gov/usaidasean/ (accessed 5 September 2024).

[194] Bangkok Post (2024), ASEAN-Japan Cybersecurity Meeting Boosts Regional Collaboration. https://www.bangkokpost.com/thailand/pr/2737396/asean-japan-cybersecurity-meeting-boosts-regional-collaboration (accessed 5 September 2024).

related technologies.

APT40 engages in spear-phishing, deploying specialised malware for intrusion, and exploiting software vulnerabilities. These tactics are designed to infiltrate systems and extract sensitive information, potentially destabilising national security.

Figure A.65 Overview of Cybersecurity in Indonesia



Source: Created by authors.

Other than APT, darknet exposure is also considered as another major cyberthreat in Indonesia. Darknet exposure is a condition when there is data or information on account credentials at a particular organisation that is exposed on the darknet. Darknet exposure can be caused by a malware stealer infection on a user's device, or by theft/dump of an organisation's database. The number of data breached in Indonesia had been increasing significantly since 2021 to 2023, from 84,000 data breached to more than 1.6 million data breached. This is mostly caused by darknet exposure. In 2023, the energy and mining sectors accounted for 5.18% of major cyber incidents, highlighting the sector's vulnerability to significant cyber-attacks. Approximately 1.75% of the Darknet exposure related to compromised credentials in 2023 was attributed to the energy and mining sectors[195]. This exposure involves stolen credentials being traded on the Darknet, posing further security risks.

Data leakage incidents within the energy sector represented about 2.3% of all data leakage incidents in 2023. These leaks can have severe consequences for the confidentiality and integrity of sensitive information.

[195] Badan Siber dan Sandi Negara-BSSN (2023) , Lanskap Keamanan Siber 2023. Jakarta . https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf

Table A.16 Cybersecurity Incidents in Different Sectors

Sectors	Number of Cyber Incidents *alleged	Number of Darknet Data Exposure	Number of Data Leakage Incidents
Government Administration	186	665,916	71
Others	60	586,597	12
Finance	38	165,085	12
Transportation	24	161,282	1
Energy and Mining	18	56,925	3
ICT	5	29,350	1
Healthcare	5	3,785	1
Food and Agriculture	5	3,287	1
Defense	2	1,958	1
Total	347	1,674,185	103

Source: Created by authors based on BSSN's 2023 Annual Report

Table A.17 Notable Cases of Cyberattacks on DES in Indonesia

Type of attack	Year	Incident	Overview	Impact
Ransomware	2024	Temporary National Data Centre Breach ('PDNS') Indonesia Automatic Fingerprint Identification System (INAFIS) Indonesia National Armed Forces Strategic Intelligence Agency	In June, Brain Cipher hacker group delivered numerous cyber-attacks to major several government agencies. This attack exposed the vulnerability of Indonesia's data security systems.	Numerous government agencies, roughly 300 central and local agencies were halted. Immigration services partially restored in CGK International airport Massive public outrage which prompted resignation of the ICT Minister to resign.
Malware	2022	Ministry of Communication and Informatics Data Leakage ('Bjorka')	A hacker named 'Bjorka' performed cyber attacks to Ministry of Communication and Informatics infrastructure which led to numerous personal data to be sold in public forums	150 million of personal data were leaked, which also include high-ranking government officers. 1.3 million SIM Card Data Top-secret letter from National Intelligence Agency to The

				President was leaked.
Ransomware	2023	Indonesia Islamic Bank Data Theft	A hacker called 'Lockbit' delivered a ransomware attack to Indonesia Islamic Bank ('BSI')	1.5 TB worth of data was stolen which also included 15 million customers account including passwords, personal data and financial information.
Malware	2020	Tokopedia Data Leakage	In March 2020, Whysodank performed cyber attack on Tokopedia and sold the personal data on public forums.	There are 91 million user accounts, and 7 million merchants account were stolen and sold in public forums.

Source: Created by authors from various news articles.

In 2023, Indonesia experienced a major cybersecurity incident when a ransomware attack targeted the nation's National Data Centre (PDNS) and several armed forces agencies. This breach, attributed to the Brain Cipher hacker group, exposed significant vulnerabilities in Indonesia's data security systems[196]. The attack disrupted operations across approximately 300 central and local government agencies, leading to halted functions in crucial areas. Amongst the affected services were immigration operations at Soekarno-Hatta International Airport (CGK), which were only partially restored, causing widespread operational delays. The scale of the breach resulted in significant public outrage, culminating in the resignation of Indonesia's Minister of Information and Communication Technology (ICT). This breach not only highlighted the fragility of the nation's cybersecurity infrastructure but also underscored the pressing need for stronger data protection measures.

Another prominent cybersecurity breach involved the hacker known as 'Bjorka,' who targeted the Ministry of Communication and Informatics[197]. This attack resulted in a massive data leak, with personal information such as identification numbers and addresses being sold on public forums. The breach severely undermined public trust in the government's ability to protect citizen data and demonstrated the escalating threat of cyber espionage in Indonesia.

These incidents collectively illustrate the growing risks faced by Indonesia's digital infrastructure and the critical need for enhanced cybersecurity measures to prevent future breaches.

[196] Asia Pacific Foundation of Canada (2024), Indonesian Government Under Fire Following String of Cyber Breaches. https://www.asiapacific.ca/publication/indonesian-government-under-fire-after-cyber-breaches (accessed 18 August 2024).

[197] Liputan 6 (2022), 11 Fakta Hacker Bjorka yang Retas Data Pemerintah Indonesia. Jakarta. https://www.liputan6.com/citizen6/read/5067854/11-fakta-hacker-bjorka-yang-retas-data-pemerintah-indonesia?page=2 (accessed 28 August 2024).

(2) Government Structures related to Cybersecurity for DES

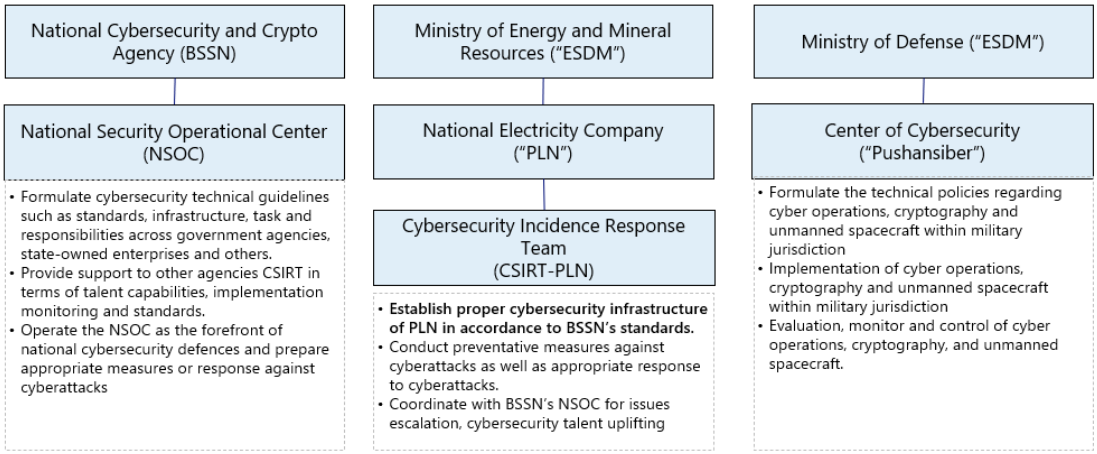
As the leading entity in cybersecurity development in Indonesia, the National Cybersecurity and Crypto Agency (BSSN) collaborates with major government bodies and state-owned enterprises to establish Cybersecurity Incident Response Teams (CSIRTs). BSSN, a government agency directly under the President's authority, was founded under Presidential Regulation Number 28 of 2021. Its primary responsibility is to oversee the policy formulation, implementation, and operation of national cybersecurity and encryption efforts across the country.

BSSN's key responsibilities include formulating technical guidelines for cybersecurity that apply to various stakeholders such as government agencies, private enterprises, and related organisations. In addition to policymaking, the agency plays a critical role in shaping the strategic direction of Indonesia's cybersecurity landscape, ensuring that the country is well-prepared to defend against evolving cyber threats. One of the agency's most crucial roles is operating the National Security Operational Command, which monitors and responds to cyber threats in real time. Furthermore, BSSN is dedicated to fostering cybersecurity talent through various improvement initiatives. These programmes target government agencies, state-owned enterprises, and academic institutions, aiming to enhance the nation's overall cybersecurity capabilities. Through these efforts, BSSN not only protects critical infrastructure but also builds a robust and skilled cybersecurity workforce to meet future challenges.

The Ministry of Energy and Mineral Resources oversees Indonesia's National Electricity Company (PLN), which has established its own Cybersecurity Incident Response Team (CSIRT-PLN). This team plays a crucial role in ensuring the cybersecurity infrastructure of PLN is in full compliance with BSSN's standards. CSIRT-PLN is responsible for implementing preventative measures to safeguard against cyberattacks and ensuring an effective response when such incidents occur.

Additionally, CSIRT-PLN works closely with BSSN's National Security Operational Command (NSOC) for issue escalation and more complex cybersecurity challenges. As part of its broader mandate, CSIRT-PLN is also involved in cybersecurity talent development, collaborating with BSSN to uplift and enhance the skillsets of its workforce to meet emerging cybersecurity threats.

Figure A.66 Overview of Related Organisations



Source: Created by authors based on PLN website[198] and Expert Interviews

(3) Policies on Cybersecurity for DES

The launch of PLN-CSIRT (Cyber Security Incident Response Team) aligns with the Indonesian government's mandate to protect vital infrastructure, as outlined in the presidential regulation. As PLN (Perusahaan Listrik Negara) is critical infrastructure due to its role in power generation, it is essential to safeguard its systems against cyber threats. The primary objective of PLN-CSIRT is to independently handle cybersecurity incidents, applying appropriate countermeasures to mitigate cyberattacks. This initiative is also a key component of PLN's broader digitalisation efforts, which span the entire electricity supply chain, from power generation to transmission, distribution, and consumption. By strengthening its cybersecurity posture, PLN ensures the resilience of its digital infrastructure and the continuity of its operations.

The increasing digitalisation in Indonesia has prompted BSSN (National Cyber and Crypto Agency) to emphasise the importance of Cybersecurity Incident Response Teams (CSIRT) in combating cyberattacks and implementing preventative measures. BSSN has already collaborated with major government agencies and state-owned enterprises to establish CSIRTs, which are designed to help organisations respond effectively to cyber incidents and implement preventive cybersecurity practices.

BSSN, through its NSOC, supports PLN in establishing PLN-CSIRT to enhance its cybersecurity capabilities[199]. PLN-CSIRT, mandated by the government to protect vital infrastructure, aims to independently manage cyber incidents, supporting PLN's

[198] PLN

[199] PLN (2022), Dukung Transformasi Digital, PLN dan BSSN Perkuat Pembentukan Tim Tanggap Insiden Siber Pertama di Sektor Energi. Jakarta. https://web.pln.co.id/cms/media/2022/07/dukung-transformasi-digital-pln-dan-bssn-perkuat-pembentukan-tim-tanggap-insiden-siber-pertama-di-sektor-energi/ (accessed 12 September 2024).

digitalisation efforts from power generation to consumption. BSSN provides technical guidelines on standards, procedures, and components for the CSIRT and assists with routine communication, reporting, and cybersecurity improvements. In the event of cyberattacks, NSOC may offer joint support based on the severity. PLN-CSIRT is responsible for implementing these guidelines, conducting cyber response planning, and performing simulations for incident response and business continuity.

(4) Guidelines on Cybersecurity for DES

BSSN Regulation Number 4 Year 2022 dictate the guidelines for information security management of electronic-based government systems including its technical standards and security procedures of electronic-based government systems. These guidelines focus on enhancing information security on electronic-based government systems (e-gov) such as online tendering platform ('LPSE') via establishment of information security standards. Central and provincial government agencies are mandated to follow these guidelines.

Under discretion aspect, the main security procedures are establishing the information classification, implement encryption-based cryptography system and access limitation for data & information based on employee levels. Regarding originality aspect, the main security procedures are provision of verification mechanism, validation mechanism and hash function system. In terms of integrity aspect, the main security procedures are applying modification detection system and verified e-signature. For denial, the main security procedures are e-signature verification and electronic certificate guarantee by organiser. Lastly for availability aspect, the main security procedures are implementation of routine back-up system, ensuring data and information accessibility and establishing recovery system.

This regulation only affects the government agencies in energy sector specifically on its electronic-based systems. For instance, Ministry of Energy and Mineral Resources application such as One Stop Monitoring System of electricity, permits and licenses online platforms, online tendering platform and many more. As DES will require permits or licenses from provincial government agencies to operate in certain areas, this regulation certainly affect that government agency.

The technical standards and security procedures for electronic-based government systems are applied in topics such as data and information security, e-gov application security, government service connector system ('SPLP') security, intra-network security and National Data Centre Security (specific on Ministry of ICT). Furthermore, there are five aspects for this technical standard such as discretion, originality, integrity, denial and availability.

Furthermore, due to increasing digitalisation, BSSN also recognises Cybersecurity Incident Response Teams (CSIRTs) as essential in combating cyberattacks and implementing preventive measures. BSSN has collaborated with major government

agencies and state-owned enterprises to establish CSIRTs, which help organisations respond to cyberattacks and implement preventive cybersecurity protocols.

BSSN, along with the Ministry of Communication and Informatics, leads the development of cybersecurity technical guidelines and standards for stakeholders across government, state-owned, and private sectors. One key initiative is the cybersecurity governance of vital infrastructure. PLN, through its subsidiary Nusantara Power (formerly PJB), partnered with BSSN to launch its CSIRT, making it the first energy company to implement a cybersecurity response system.

Besides these guidelines by the BSSN, there are also other initiatives led by government agencies. For example, the Ministry of Energy and Mineral Resources (ESDM) worked with BSSN to form a CSIRT in 2021, focusing on coordinating with the National Cybersecurity Response Team to handle cyber incidents affecting ESDM's IT infrastructure[200].

BSSN provides cybersecurity guidelines, including the Information Security Management System for government agencies (BSSN Regulation No. 4, 2021), which outlines key cybersecurity measures. Additionally, the National Cybersecurity Guidelines (Ministry of Defence Regulation No. 82, 2014) set the framework for national cybersecurity, covering stages like prevention, threat analysis, defence mechanisms, and countermeasures.

The Presidential Regulation Number 82 Year 2022 regarding Protection of Vital Information Infrastructure outlines a broad strategy for cybersecurity resilience and coordination between government entities.

Specifically, energy is one of the key sectors that is covered in this policy, due to its vital infrastructure. The policy forces key stakeholders in Energy sector to form Cybersecurity Incidence Response Team. The Cybersecurity Incidence Response Team (CSIRT) is responsible for the protection and applying appropriate measures in the case of cyberattacks.

Energy stakeholders like Ministry of Energy and Mineral Resources and PLN will create its own CSIRT division. MEMR's CSIRT falls under the Sectoral Category and PLN's CSIRT falls under Organisation Category. BSSN leads the National CSIRT where it coordinates with Sectoral CSIRT like MEMR and Organisation CSIRT like PLN in the case of cyberattacks. Furthermore, this regulation mandates information and sharing analysis centre which allows Organisation CSIRT like PLN to collaborate and communicate with BSSN to improve their cybersecurity capabilities.

DES companies like microgrid providers, off-grid power companies or similar companies cannot implement its own cybersecurity standards. These companies need to adhere with cybersecurity guidelines that are laid out by BSSN. In terms of risk prevention, BSSN also

---

[200] Kementerian ESDM (2021), Gandeng BSSN, Kementerian ESDM Bentuk Tim Tanggap Insiden Siber. Jakarta. https://www.esdm.go.id/id/media-center/arsip-berita/gandeng-bssn-kementerian-esdm-bentuk-tim-tanggap-insiden-siber (accessed 8 September 2024).

involves in establishing the CSIRT and the overall cybersecurity framework in DES companies as well as helping them in potential threats detection.

(5) Initiatives or Case Studies on Cybersecurity for DES

There are several international initiatives that have supported Indonesia in strengthening its cybersecurity capabilities through partnerships and knowledge exchange.

Developed countries such as the USA, the United Kingdom, and Australia have played a key role by sharing expertise, engaging in research and development, and conducting joint operations with Indonesia. In November 2023, the USA–Indonesia collaboration expanded under a new defence cooperation plan, where the US military committed to assisting Indonesia in enhancing its cybersecurity and space capabilities[201]. This effort is part of a broader initiative to address ASEAN countries' cybersecurity vulnerabilities.

Figure A.67 Supporting Initiatives from Developed countries

United States	• In November 2023, The USA-Indonesia expanded its collaboration on the new defence cooperation plan. **The US military will help Indonesia's military in improving its cybersecurity and space capabilities.** This was part of larger effort to improve ASEAN countries' vulnerabilities on cyber defence. • In June 2024, The US Department of Homeland Security (DHS) partnered with Government of Indonesia for maritime cybersecurity improvement in the Indo-pacific region. **The agreement aims to fortify cybersecurity measures and safeguard maritime critical infrastructure against cyber intrusions and attack**. This partnership also allowed for stress test regarding cyber incident response.
United Kingdom	• In June 2023, Foreign, Commonwealth, and Development Office (FCDO) established cybersecurity cooperation with the National Cyber and Cryptography of Indonesia. This agreement generated eight areas of cooperation such as National Cyber Strategy Development and Implementation, Cyber Threat Landscape, Cyber Governance, Government and Industry Partnership, Incident Management, Cybercrime, Promotion of Cybersecurity Awareness, Capacity Building through knowledge transfer and research.
Australia	• Indonesia and Australia cooperated **cybersecurity agreement.** The goal for this cooperation is to share best practices and utilization of emerging cyber technology cooperation. **Australia views Indonesia as a powerhouse for digital economy in ASEAN but cyber resilience improvement is still the main issue.** The country still lacks digital talent to support Indonesia's ICT infrastructure.
China	• PLN formed collaboration with State Grid Corporation of China (PLN-SGCC Partnership) to **boost clean energy development via collaborative studies on power grid integration**, smart grid management, and electric power storage. The PLN and SGCC will work together on developing Smart Grid as the backbone of clean energy electricity in Indonesia.

Sources: Created by authors based on various news articles.

For instance, in June 2024, the U.S. Department of Homeland Security (DHS) partnered with the Indonesian government to enhance maritime cybersecurity in the Indo-Pacific region [202]. The agreement focuses on improving defences for maritime critical infrastructure against cyber threats and conducting stress tests to assess the effectiveness of incident response systems.

The United Kingdom has also contributed to Indonesia's cyber resilience efforts. In June

[201] DefenseOne (2023), US, Indonesia expand defense cooperation, starting with cyber and space. USA. https://www.defenseone.com/defense-systems/2023/11/us-indonesia-expand-defense-cooperation-starting-cyber-and-space/392104/ (accessed 20 August 2024).

[202] Industrial Cyber (2024), US DHS partners with Indonesia to strengthen maritime cybersecurity in Indo-Pacific region. https://industrialcyber.co/transport/us-dhs-partners-with-indonesia-to-strengthen-maritime-cybersecurity-in-indo-pacific-region (accessed 18 August 2024).

2023, the UK's Foreign, Commonwealth, and Development Office (FCDO) entered into a cybersecurity cooperation agreement with Indonesia's National Cyber and Crypto Agency (BSSN)[203]. This collaboration covers eight key areas: National Cyber Strategy Development, Cyber Threat Landscape, Cyber Governance, Government and Industry Partnerships, Incident Management, Cybercrime, Cybersecurity Awareness, and Capacity Building through knowledge sharing and research.

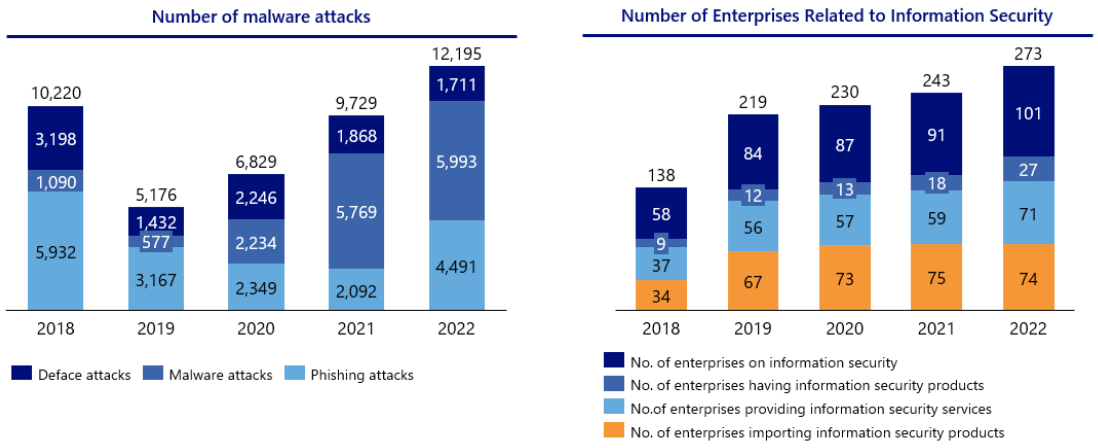
These international partnerships reflect Indonesia's ongoing efforts to fortify its cyber defences in response to an increasingly digitalised and interconnected world.

1-2-6. Viet Nam

(6) Overview on Cybersecurity

Viet Nam's cybersecurity landscape has faced significant challenges in recent years, marked by fluctuating attack trends. However, the country is gradually maturing in this sector, with increasing diversity in cybersecurity roles and a growing capacity to address emerging threats.

Figure A.68 Overview of Cybersecurity in Viet Nam



Source: Ministry of Information and Communications[204]

One of the most notable trends is the significant rise in malware attacks, which surged from 1,090 in 2018 to nearly 6,000 in 2022, suggesting that Viet Nam has become a more prominent target or that malware tactics have evolved. Phishing attacks, after an initial decline from 5,932 in 2018 to 2,092 in 2021, experienced a resurgence in 2022, with the number rising to 4,491. This indicates a renewed threat, likely driven by evolving tactics

[203] OpenGovAsia (2023), Indonesia and UK Strengthen Cybersecurity Cooperation. Jakarta . https://opengovasia.com/2023/06/30/indonesia-and-uk-strengthen-cybersecurity-cooperation/ (accessed 20 August 2024).

[204] Ministry of Information and Communications (2023), Sách trắng TÁ 2023. https://mic.mediacdn.vn/63935241018719846 4/2024/8/22/sach-trang-ta-2023-7-6-24-17243135905472033515302.pdf (accessed 5 September 2024).

employed by cybercriminals. Deface attacks, which involve altering website content, saw a decline over the years, from 3,198 in 2018 to 1,711 in 2022.

The combination of rising cyberattacks and a rapidly expanding cybersecurity industry demonstrates Viet Nam's evolving approach to addressing its digital security challenges.

Figure A.69 Notable Cases of Cyberattacks on DES in Viet Nam

Type of DES	Type of attack	Year	Incident	Overview	Impact
NA	Ransom ware	2024	Vietnam's state oil distribution firm PetroVietnam Oil Corp (PV Oil) reported that its information technology system was deliberately and illegally targeted with ransomware	PV Oil was hit by a ransomware attack at midnight, disrupting its information technology systems.	Affected over 780 petrol stations nationwide, including the company's electronic invoicing, email, and business portal systems, forcing a temporary suspension of electronic invoicing.
NA	Ransom ware	2023	On December 4, 2023, it was reported that the BlackCat ransomware group, targeted Ho Chi Minh City Energy Company, a subsidiary of Vietnam Electricity (EVN)	Despite the severity of the attack, EVN's website remains operational with no immediate signs of disruption.	The hackers have posted 84 samples of the stolen data on the dark web. EVN is Vietnam's largest power company, managing a significant portion of the nation's power generation.
NA	Data breach Website defacem ent	2016	Chinese hackers attack VN's airports and Vietnam Airlines' website	Chinese hacker group, 1937CN, launched cyberattacks on Vietnam's two largest airports, Noi Bai and Tan Son Nhat, as well as the official website of Vietnam Airlines.	The attacks included offensive messages on airport screens about the South China Sea dispute, distorted announcements at Noi Bai airport, and the replacement of the Vietnam Airlines website with similar content, along with a customer database leak.

Source: Tuoi Tre News[205], Vietnam News[206]

Viet Nam has experienced several significant cyber incidents that have raised concerns about its cybersecurity infrastructure, particularly in critical sectors like energy and aviation. As the country with the 12th largest internet user population globally, it faces growing vulnerabilities, with many cyberattacks linked to foreign entities, including Chinese hackers[207].

For instance, PV Oil, Viet Nam's state oil distribution company, reported a ransomware attack on its IT systems. The attack was a deliberate and illegal targeting of the firm's infrastructure, highlighting vulnerabilities in the energy sector[208]. This incident raised alarms about the potential impact of such attacks on national security and critical operations.

---

[205] Tuoi Tre News (2024), Petrovietnam Oil Corp hit by ransomware attack. https://tuoitrenews.vn/news/business/20240403/petrovietnam-oil-corp-hit-by-ransomware-attack/79151.html (accessed 5 September 2024).

[206] Vietnam News (2016), Chinese hackers attack VN's airports and Vietnam Airlines' website. https://vietnamnews.vn/society/300416/chinese-hackers-attack-vns-airports-and-vietnam-airlines-website.html (accessed 5 September 2024).

[207] Duong Ngoc Thai (2020), Vietnam has no choice but to counter China's cyber thuggery. https://e.vnexpress.net/news/perspectives/vietnam-has-no-choice-but-to-counter-china-s-cyber-thuggery-4107109.html (accessed 5 September 2024).

[208] Tuoi Tre News (2024), Petrovietnam Oil Corp hit by ransomware attack.

Additionally, Ho Chi Minh City Energy Company (EVN), on December 4, 2023, the BlackCat ransomware group targeted the Ho Chi Minh City Energy Company, a subsidiary of Vietnam Electricity (EVN). This attack on an essential energy provider underscored the risks faced by Viet Nam's energy infrastructure from sophisticated cybercriminals.

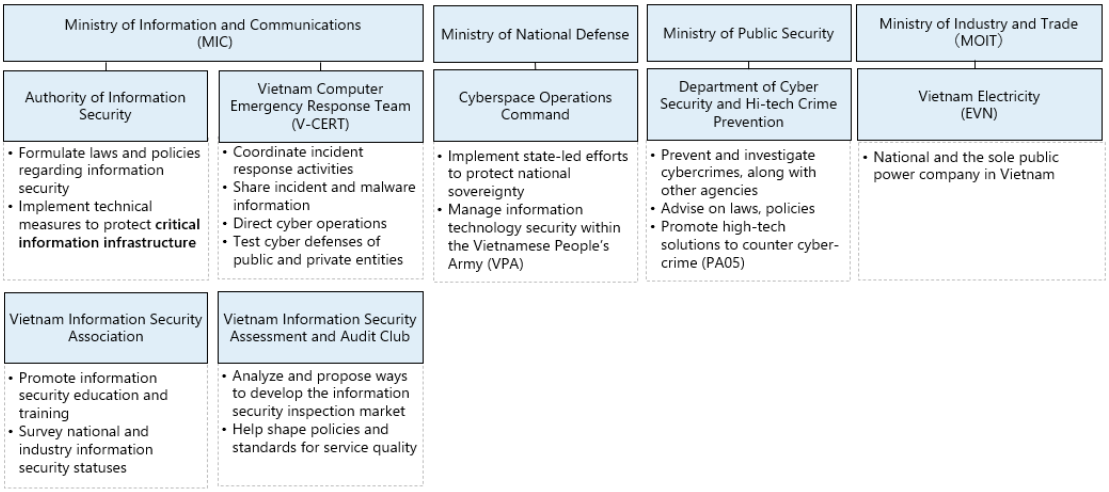
In another high-profile incident, Vietnam Airlines' website and the country's airports were attacked by Chinese hackers[209]. This breach not only disrupted services but also raised concerns about national sovereignty, given that aviation infrastructure is critical for national security and economic stability.

(7) Government Structures related to Cybersecurity for DES

In Viet Nam, the Authority of Information Security and the Vietnam Computer Emergency Response Team (V-CERT) play pivotal roles in enhancing the country's cybersecurity, particularly in the protection of its Critical Information Infrastructure (CII). Given the frequent cyberattacks often attributed to Chinese hackers, Viet Nam faces significant vulnerabilities that raise concerns about national sovereignty, security, and domestic stability. Amongst ASEAN Member States, Viet Nam and Thailand are recognised for their superior cyber resilience, especially in incident response. Viet Nam's advanced national-level cyber incident detection and response units are notably more effective compared to those in other ASEAN countries.

[209] Vietnam News (2016), Chinese hackers attack VN's airports and Vietnam Airlines' website.

Figure A.70 Overview of Related Organisations



Source: International Institute for Strategic Studies[210], Ministry of Information and Communications (MIC)[211], Vietnam Information Security Association (VNISA) [212], The Diplomat [213], People's Public Security Newspaper[214], Vietnam Information Security Association (VNISA)[215]

Under the Ministry of Information and Communications (MIC), the Authority of Information Security is responsible for formulating laws and policies related to information security and implementing technical measures to safeguard critical infrastructure. V-CERT, on the other hand, focuses on operational aspects of cybersecurity. It coordinates incident response activities, shares information on malware and cyber incidents, directs cyber operations to address real-time threats, and tests the cyber defences of both public and private entities. Together, these agencies are central to Viet Nam's cybersecurity framework, ensuring that the country can effectively respond to and mitigate the impact of rising cyber threats.

---

[210] International Institute for Strategic Studies (IISS) (n.d), Cyber capabilities and national power: Vietnam. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---vietnam.pdf (accessed 5 September 2024).

[211] Ministry of Information and Communications (MIC), Vietnam (n.d), Authority of Information Security. https://english.mic.gov.vn/authority-of-information-security-197114301.htm (accessed 5 September 2024).

[212] Vietnam Information Security Association (VNISA) (n.d), Cybersecurity Emergency Response Center established. (accessed 5 September 2024).

[213] The Diplomat (2018), What's Behind Vietnam's New Military Cyber Command?. https://thediplomat.com/2018/01/whats-behind-vietnams-new-military-cyber-command/ (accessed 9 September 2024).

[214] People's Public Security Newspaper (2020), Department of Cyber Security and Hi-tech Crime Prevention Requested to Effectively Prevent Cyber Crimes. https://en.cand.com.vn/public-security-forces/Department-of-Cyber-Security-and-Hi-tech-Crime-Prevention-requested-to-effectively-prevent-cyber-crimes-i549548/ (accessed 9 September 2024).

[215] Vietnam Information Security Association (VNISA) (n.d), About VNISA. https://vnisa.org.vn/en/about-vnisa/ (accessed 9 September 2024).

(8) Policies on Cybersecurity for DES

Viet Nam is making significant strides to enhance its cybersecurity posture through a comprehensive national strategy and regulatory framework. While there is currently no specific policy or guideline addressing cybersecurity for Distributed Energy Systems, Viet Nam's overarching cybersecurity strategy aims to improve its Global Cybersecurity Index (GCI) ranking. The strategy's key focus areas include strengthening state management of cybersecurity, refining legal frameworks, protecting national sovereignty in cyberspace, securing digital infrastructure, and safeguarding critical information systems.

Viet Nam's cybersecurity strategy focuses on improving its Global Cybersecurity Index (GCI) ranking by enhancing state management, refining legal frameworks, protecting national sovereignty in cyberspace, securing digital infrastructure, and safeguarding critical information systems. Key targets include maintaining or improving its GCI ranking by 2025 and enhancing digital trust by 2030.

The Cybersecurity Administrative Sanctions Decree (CAS Decree), aimed at strengthening data protection for both local and foreign entities, introduces penalties for data breaches, with fines up to 5% of an organisation's revenue in Viet Nam for violations such as unlawful data processing and non-compliance with data transfer rules. Additional penalties may include revoking permits or licenses. Although initially planned for June 2024, the decree is still under revision.

(9) Guidelines on Cybersecurity for DES

One significant regulatory measure is the Cybersecurity Administrative Sanctions Decree (CAS Decree). Although initially drafted in September 2021 and revised through public consultations, the CAS Decree is scheduled to take effect on June 1, 2024, pending further revisions. The CAS Decree aims to bolster cybersecurity and data protection for both Vietnamese and foreign entities operating in Viet Nam. It imposes stringent penalties for various breaches, including fines of up to 5% of an organisation's total revenue in Viet Nam for repeated unlawful processing of personal data, unlawful data handling, failure to submit a personal data processing impact assessment, and non-compliance with international data transfer obligations. Additional penalties may include the revocation or suspension of permits, certificates, or licenses, underscoring Viet Nam's commitment to enhancing its cybersecurity and data protection measures.

(10) Initiatives or Case Studies on Cybersecurity for DES

Viet Nam's Information and Communication Infrastructure Master Plan, outlined in Decision 36/QD-TTg and approved by Prime Minister Phạm Minh Chính, presents a strategic framework for advancing the country's digital infrastructure with a strong focus on cybersecurity. The plan aims to position Viet Nam as a leading network security hub in

Asia by 2030.

Figure A.71 Viet Nam's Digital Infrastructure Master Plan to 2030

Year	Development Requirement	Description
2025	Digital Trust	**Establish a trustworthy and healthy cyber environment. Develop a comprehensive People's Security Strategy capable of coordinating and addressing harmful information.**
	Securing State Information Systems	Ensure all state agency information systems are secure, and all ministries and **local authorities implement network security measures**.
	Professional Units and Tools	Each entity should have a **professional network security** unit and every citizen should have at least one network security tool.
	Market Growth	Aim for a **20-30% annual growth in network security market revenue**.
	Awareness and Ranking	Ensure 100% of internet users have access to information and **tools for network security**. Maintain a top 25-30 position in the Global Cybersecurity Index.
	Product Ecosystem	Achieve a diverse network security product ecosystem, with 3-5 key products dominating the domestic market and competing internationally.
2030	Regional Leadership	Position Vietnam **as a leading center for network and cybersecurity in Asia**.
	Market Formation	Develop a competitive network security market with influence across the region and globally. Encourage the use of open source technologies and ensure Vietnamese enterprises lead in this market.

Source: Vietnam Briefing[216], USAID[217]

Key components of the plan include the development of high-speed internet, green data centres, and specialised IT parks. The strategy emphasises the protection of digital government operations, the economy, and society through comprehensive cybersecurity measures. This includes securing state information systems, enhancing public awareness about cyber threats, and fostering a robust ecosystem of cybersecurity products. The plan reflects Viet Nam's commitment to not only advancing its digital capabilities but also ensuring a secure and resilient cyber environment as it seeks to strengthen its role in the region's cybersecurity landscape.

[216] Vietnam Briefing (2024), Vietnam's Digital Infrastructure Master Plan to 2030: Roadmap to a High-Tech Future. https://www.vietnam-briefing.com/news/vietnams-digital-infrastructure-master-plan-2030-roadmap-to-a-high-tech-future.html/ (accessed 9 September 2024).

[217] USAID (2022), USAID supports Vietnam's innovation and digital transformation in the public sector. https://www.usaid.gov/vietnam/news/apr-8-2022-usaid-supports-vietnams-innovation-and-digital-transformation-public-sector (accessed 9 September 2024).

Figure A.72 Supporting initiatives from Foreign Countries

USAID	• USAID has advanced digital transformation in Vietnam's public sector through its Strengthening Provincial Capacity (SPC) program, which created an executive training course on digital transformation, including cybersecurity, in collaboration with Portland State University. • In 2023, USAID launched the Digital Connectivity and Cybersecurity Partnership (DCCP) in Suva with the University of the South Pacific (USP). This initiative aims to enhance digital access and security across the Pacific region by improving broadband connectivity, digital government services, and secure internet access.
Japan	• Collaboration between Japan and ASEAN member states (AMS) due to the rising threat of cyberattacks, particularly from state-sponsored actors like China, Russia, and North Korea. • Key initiatives include the ASEAN-Japan Cybersecurity Community Alliance (AJCCA) and the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC), which focus on information sharing and workforce development. • The Japan International Cooperation Agency (JICA) has funded the "Project on Cyber Building for Cyber Security in Vietnam (2019-2024)" to enhance Vietnam's cyber capabilities. This project involved certification training for cyber threat intelligence, policy planning for cybercrime investigations, and the installation of Distributed Denial of Service (DDoS) attack mitigation systems.

Source: Fulcrum[218]

Viet Nam is benefiting from several international initiatives aimed at enhancing its cybersecurity capabilities. Both Japan and ASEAN Member States have been instrumental in supporting Viet Nam's cybersecurity efforts through various programmes and collaborations.

USAID has played a significant role in advancing digital transformation in Viet Nam's public sector through its Strengthening Provincial Capacity (SPC) programme. This initiative, developed in partnership with Portland State University, includes an executive training course focused on digital transformation and cybersecurity. In addition, in 2023, USAID launched the Digital Connectivity and Cybersecurity Partnership (DCCP) in Suva, in collaboration with the University of the South Pacific (USP). This initiative aims to enhance digital access and security across the Pacific region by improving broadband connectivity, digital government services, and secure internet access.

Japan has also been active in supporting Viet Nam's cybersecurity development. The Japan International Cooperation Agency (JICA) funded the Project on Cyber Building for Cyber Security in Vietnam (2019–2024), which aims to bolster Viet Nam's cyber capabilities. This project includes certification training for cyber threat intelligence, policy planning for cybercrime investigations, and the installation of Distributed Denial of Service (DDoS) attack mitigation systems.

[218] Fulcrum (2024), Strengthening ASEAN-Japan cybersecurity cooperation. https://fulcrum.sg/strengthening-asean-japan-cybersecurity-cooperation/ (accessed 9 September 2024).