ENERGY STUDIES INSTITUTE

Policy *Brief* 9

12 November 2015

Mitigating Cybersecurity Threats to Southeast Asia's Smart Grids

Nur Azha Putra

SYNOPSIS

Singapore, Malaysia, Indonesia, the Philippines and Thailand are in the midst of test-bedding smart grids. This is taking place at a time when the world is seeing an increase in global cybersecurity attacks specifically targeted at the energy sector. Although these five nations already have cybersecurity laws and policy frameworks in place, it remains uncertain if these existing measures will be sufficient to mitigate cybersecurity threats aimed at smart grid operators and energy consumers.

KEY POINTS

- Hackers are increasingly targeting the energy sector due to the potentially high economic impact and widespread social effects; moreover, smart grids are known to be vulnerable to cyber attacks.
- Singapore, Malaysia, Indonesia, the Philippines and Thailand are in the midst of test-bedding smart grid applications.
- The governments of Southeast Asian nations should build on existing international cybersecurity regimes and ASEAN's mechanisms to mitigate potential threats to the region's emerging smart grid industry.

INTRODUCTION

According to the Institute of Electrical and Electronics Engineers (IEEE), based in New York, a smart grid is a "next-generation electrical power system that is typified by the increased use of communications and information technology in the generation, delivery, and consumption of electrical energy". Central to the deployment of smart grids is the use of metering technology such as "smart meters", which "give real time feedback to the end users on their energy usage and what it is costing them (consumers)". By replacing the traditional electrical grids and "dumb meters" with smart grids and smart meters, the overall energy generation and consumption landscape will be more reliable and energy efficient.

Consumers equipped with smart meters will better understand their energy needs and consumption patterns, and therefore become more aware of their power consumption habits. At the same time, power generators will be better able to manage their power supplies during peak and off-peak periods based on consumers' consumption profiles. In the larger scheme of things, based on the information provided through the smart meters, power generators and grid operators will be better prepared to manage their demand response. However, technology-based information communications systems such as smart grids and smart meters, while more reliable and efficient, are known to be vulnerable to cybersecurity attacks.

Energy Studies Institute
29 Heng Mui Keng Terrace,
Block A, #10-01, Singapore 119620
Tel: (65) 6516 2000 | Fax: (65) 6775 1831
esi.nus.edu.sg

A Research Institute of NUS National University of Singapore

Several Southeast Asian states are in the midst of test-bedding smart grid applications, and the region is likely to witness a smart grid "revolution" within the next decade. Since 2010, Singapore has been gradually test-bedding smart grid applications at Pulau Ubin and selected estates in Punggol, while Malaysia has been testing smart grid advance meters in Putrajaya and Malacca since 2013. Indonesia has also been running pilot projects in Jakarta, Batam, Bangka and Sumba since 2012. Similarly, the Philippines has been implementing smart grid tests in the cities of Antipolo and Taytay since 2013, while Thailand has been conducting its smart grid tests in Mae Hong Son Province since 2012. Although it will still be some years before smart grids are extensively deployed in the region, it is clear that the Southeast Asian nations are looking to use smart grids as a means to improve their energy efficiency.

ANALYSIS

Cybersecurity Threats

Security specialist firm Maxim Integrated reported in its 2013 white paper that a Puerto Rican power utility firm suffered up to USD 400 million losses when hackers altered the data in its smart meters. In its 2012 security report, the European Network and Information Security Agency, an EU agency dedicated to preventing and addressing network security, warned that hackers could use a "worm" to gain remote access to homes that have smart meters. Such examples, occurring in two different regions of the world, show the vulnerability of households and power utilities hooked up to smart grids.

To date, there have been no known cases of hacktivists, terrorists or perpetrators of organised crime issuing any threats towards the fledgling smart grid industries in Southeast Asia. However, there were three recent cybersecurity-related incidents in the region that suggest that smart grid vulnerabilities could be exploited by non-state actors motivated by inter-state conflicts.

The first incident took place in 2013 when Malaysian government websites were defaced by hackers, believed to be from the Philippines and who were disputing Malaysia's ownership of Sabah. The second incident, which also occurred in 2013, was a cyber war that erupted between hackers claiming to be from the Bangladesh Grey Hat Hackers and Indonesia's Cyber Army. For several months, both sides hacked into and defaced Bangladeshi and Indonesian websites. The third incident took place that same year, when the website of Eu Yan Sang, a Singapore-based company specialising in traditional Chinese medicine (TCM) products and services, was defaced by hackers claiming to be from Indonesia. In the message they posted, the perpetrators explained that the attack was in retaliation to the Singapore government's position towards Indonesia on the issue of the transboundary haze.

Types of Smart Grid Threats

Presenters at the 2010 International Conference on Smart Grid Communications, organised by IEEE, warned that by 2015, global smart grids would be vulnerable to at least 440 million potential points of attack. This number is likely to rise dramatically with the increasing use of communications devices and home appliances connected to the Internet.

As highlighted on the *Security Intelligence Blog* of TREND Micro, a global Internet security corporation, smart grids could be attacked in many different scenarios and for different purposes. For instance, if their aim is to disrupt normal services, hackers would launch a denial-of-service attack by inserting corrupt data into the computer servers of the electricity retailers. This could cause the computer servers to malfunction and become unable to accurately process the information that that they receive and send to the grid. In addition, cyber attackers could easily manipulate power-grid data by intercepting communications between substations, grid operators, electricity consumers and suppliers.

There are several types of cyber attackers, namely business competitors, organised criminal syndicates, terrorists, hacktivists, or even disgruntled employees. Hackers could target grids in order to manipulate the data exchanges in smart grids and influence the electricity market. According to TREND Micro, electricity bill manipulation could be achieved through the electronic tampering of smart meters. Hackers could modify the information that is released by the end-user smart meters, and the discrepancies in the information sent (by the smart meters) and received by the retailers could lead to errors in the electronic bills of electricity consumers.

Getting hold of information passed between electricity retailers and energy consumers makes it easy for hackers to carry out crimes like robbery and extortion. For instance, the data generated by the smart meter could be used to determine the different types of electronic appliances that are being utilised by the end user. That same information could then be used to identify the end user's consumption pattern, such as which parts of the day or night a homeowner or factory staff is unlikely to be on the premises. Such information could be used by hackers to determine their best opportunity to commit burglary and theft.

With access to electricity consumption pattern data, hackers could also determine when corporations are in most need of an uninterrupted power supply. They could then leverage on such information to extort corporations by threatening to cut off the power supply via remote control.

Southeast Asian States: National Responses

In 2015, Singapore's government designated a Minister to head the newly created Cyber Security Agency (CSA), and made the power sector one of its priority concerns. The CSA's role is to create "a robust infocomm ecosystem" through collaborations with the public and private sectors, in addition to managing the country's cybersecurity defence, incident detection and response. The government also intends to develop its infocomm security manpower by investing heavily in its related training and education.

In Malaysia, the government has included the energy sector in its national cybersecurity framework and prioritised it as one of its "Critical National Information Infrastructures". It has also established CyberSecurity Malaysia, an agency specialising in providing technical guidance, support and consultancy services to companies and government agencies, in addition to public education and outreach.

Indonesia's internet governance model leans towards a public–private partnership. Its Ministry of Communication and Information directly manages the cybersecurity practices of its agencies while collaborating with the private sector, including energy companies, to enhance emergency preparedness and response.

The government of the Philippines enforces cybersecurity through the Philippine National Police's Anti-Cybercrime Group (PNP-ACG), which oversees the country's response to cybersecurity incidents, including cases that occur in the energy sector. The PNP-ACG's aims are: Regulation, Competence and Capacity-Building, Public–Private Partnership, International Cooperation and Advocacy. However, there appears to be no specific strategy to mitigate cybersecurity threats to smart grids.

Of all the Southeast Asian states with smart grid aspirations, Thailand seems to be the least prepared and equipped with policy tools. The Thai government, which is still in the midst of revising its 2015 National Cybersecurity Bill draft, appears to be focused instead on protecting the country's burgeoning digital economy and increasing electronic commerce activities.

Generally, there seems to be a conscious effort by the Southeast Asian governments to

mitigate cybersecurity threats to their energy sectors and infrastructures. However, it remains unclear if existing national and regional cybersecurity strategies and policy mechanisms will be sufficient to protect smart grids. As it stands, none of the Southeast Asian states that are actively test-bedding smart grid technologies has cybersecurity policies or strategies solely for smart grid protection.

Cooperation in Southeast Asia?

In addition to embedding specific smart grid protection strategies into the national cybersecurity policy framework, the governments of Southeast Asia need to engage in cyber diplomacy to strengthen the region's collective capacity to respond to smart grid cybersecurity threats. For example, the countries could participate in international internet governance treaties such as the 2001 Budapest Convention on Cybercrime. This is a comprehensive rules-based global internet governance regime which seeks "a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation". As of 2015, the Philippines is the only Southeast Asian state included in the Budapest Convention.

In addition, the Southeast Asian states could build upon existing Association of Southeast Asian Nations (ASEAN) mechanisms, such as the "Senior Official Meeting on Transnational Crime Working Group on Cybercrime" and the "ASEAN Regional Forum Statement on Cooperation in Ensuring Cyber Security". Since these focus on broad cybersecurity threats without addressing specific threats to vulnerable sectors such as smart grids, a cybersecurity smart grid working group under ASEAN's leadership could be formed to identify the actors and map out the threat vector of cybersecurity attacks on smart grids.

CONCLUSION

Governments throughout the world need to collaborate more closely to protect their critical energy infrastructure such as smart grids. The international response has been less than successful, given the general reluctance to arrive at a common internet governance framework due to differences in national priorities and state ideologies. In Southeast Asia, the governments typically express enthusiasm about regional cooperation but are struggling to harmonise dissimilar national cybersecurity policy frameworks, policy priorities and threat mitigation strategies. Ideally, they need to join efforts with not only the law enforcement agencies, but also the various stakeholders such as the utility companies and the smart grid vendors. Issues for discussion could include alignment of priorities against cybercrime threats, information-sharing, coordination for cross-border cybercrime investigations, the hiring of cyber liaison officers, and establishing a common resource pool of experts and analysts.

WHAT TO LOOK OUT FOR

- The level of resources that the various Southeast Asian governments will allocate towards the protection of critical energy infrastructure, such as smart grids.
- If cybersecurity will be discussed at the ASEAN Summit and among government agencies.

Nur Azha Putra is a Research Associate at the Energy Studies Institute of the National University of Singapore.