Jurnal Pertahanan
Media Informasi tentang Kajian dan Strategi Pertahanan
yang Mengedepankan Identity, Nationalism, & Integrity
e-ISSN: 2549-9459
Journal Homepage : http://jurnal.idu.ac.id/index.php/DefenseJournal

BRUNEI DARUSSALAM'S E-GOVERNMENT STRATEGY IN OVERCOMING CYBER THREATS

Mahendro Bhirowo[1], *Indonesia Defense University, mahendrobhirowo@idu.ac.id*
Fauzia Gustarina Cempaka Timur[2], *Indonesia Defense University, Indonesia,*
Mardi Siswoyo[3], *Indonesia Defense University, Indonesia*

Article Info

Article history:
Received 18 September 2018
Revised 19 October 2018
Accepted 19 October 2018

Keywords:
Brunei,
Cyber threat,
E-Government

Abstract

E-Government is a government administration system that plays a vital role in the international global communication, and greatly determines the progress of a state. However, the government administration system that utilizes Information and Communication Technology may be exposed to threats, especially threats originating from cyberspace. This research was carried out with the aim to analyze Brunei Darussalam's E-Government strategy in overcoming cyber threats. This study uses descriptive qualitative research methods accompanied by data obtained from the presentations and interviews during the overseas field study visits in Brunei Darussalam by the representatives of the Ministry of Foreign Affairs and Trade (MOFAT), IT Protective Security Services (ITPSS), and the Prime Minister's Office (PMO) of Brunei Darussalam, as part of a research related to Brunei Darussalam's e-Government strategy in overcoming cyber threats. The results of this study indicate that the Brunei Darussalam's e-Government strategy in overcoming cyber threats was carried out by focusing on citizen-centric service delivery in stages. It begins with the establishment of a law on computer abuse in 2000, followed by the establishment of Brunei National Computer Emergency Response Team (BruCERT) in 2004, introduction of Internet Ethics and Cyber Security Awareness Program in 2009, and the development of a national cyber security framework in 2014. All are integrated into a common policy coined as Brunei Insight 2035. This can be an input for the implementation of e-Government in Indonesia, in order to improve the equality and openness of access to information and communication in Indonesia, without neglecting the principles of security and comfort in communicating and obtaining information.

[1] Graduate Student in Cohort-5 Asymmetric Warfare Study Program of Universitas Pertahanan. email mahendrob22@gmail.com; mahendrobhirowo@idu.ac.id.
[2] Lecturer in Asymmetric Warfare Study Program of Universitas Pertahanan. Email: fgcempakatimur@idu.ac.id.
[3] Lecturer in Asymmetric Warfare Study Program of Universitas Pertahanan. Email: mardisiswoyo@idu.ac.id.

INTRODUCTION

The rapid development of the internet and information technology, especially in the 1990s, resulted in governments around the world, especially in developed states, adopting the 'Internet' in their daily lives to improve their quality of service in reaching out, socializing and communicating to the people, especially the stakeholders and interest group which includes private sector, mass media, professional groups and other civil society organizations. The contemporary dynamics of public policy related to the internet have also experienced a fairly rapid development which eventually gave birth to the concept of 'e-Government' (electronic government) which is now being adopted by many developed states, including Brunei Darussalam.

Brunei Darussalam, a state with the second highest human development index in Southeast Asia after Singapore and is classified as a developed state, has used e-Government concept to reach its people as part of its public service in Brunei Darussalam. The e-Government concept was even included in the Brunei Darussalam long-term program called the Brunei Insight 2035 which was launched by Sultan Hassanal Bolkiah (Government of Brunei Darussalam, 2015).

From the perspective of asymmetric warfare, if the e-Government program of Brunei Darussalam can be realized as planned, it can be said that Brunei Darussalam will have high immunity to asymmetric attacks. This is possible because the e-Government program of Brunei Darussalam, which also includes "One ID for citizens, One ID for businesses, Services that support One ID," will be able to map all financial transactions, as well as the movement of people and goods in Brunei Darussalam. All activities in Brunei Darussalam will be monitored electronically which means that, from the perspective of asymmetric warfare, there is potentially no undetected threat in Brunei Darussalam. This is possible because all activities in Brunei Darussalam, both in the field of business and services, are connected in the same identity which is supervised electronically. This also means that the government of Brunei Darussalam places the cyber domain as the spearhead of its military defense in the face of various asymmetrical threats, including cyber-attack. By understanding Brunei Darussalam's strategy in implementing e-Government, the Government of Indonesia can learn precious lessons in building a e-Government system in Indonesia, not only for the purpose of overcoming cyber threats, but also a variety of other threats which often use cyberspace as a medium or avenue in disrupting Indonesia's defense and security.

RESEARCH METHODS

Research design

This study uses descriptive qualitative research methods accompanied by data which is then examined through literature review and online research. Qualitative methodology is a method based on written words or verbal expression from actions that can be seen (Moleong, 2017). In line with that, Sugiyono (Sugiyono, 2016) emphasizes that qualitative research methods occur due to a paradigm shift in society over the reality.

The position of researcher is a key instrument that provides interpretation of research findings in the field. The data collection technique is done through triangulation process in data analysis. While the data analysis is done by using the Entman model of framing analysis, which prescribes that induction and research finding can provide more meaningful explanation than generalization.

The data in this study includes primary data obtained through interviews and also the exposure during a Foreign Lecture visit in Brunei Darussalam by representatives of the Ministry of Foreign Affairs and Trade (MOFAT), IT Protective Security Services

(ITPSS), and Prime Minister's Office (PMO) of Brunei Darussalam, as part of a research project related to Brunei Darussalam's e-Government strategy in overcoming cyber threats.

In addition, secondary data is also obtained from various relevant information sources regarding Brunei Darussalam's e-Government strategy in overcoming cyber threats, especially those related to the issue of asymmetric warfare.

LITERATURE REVIEW

E-Government

Mustopadidjaya (Mustopadidjaya, 2003) suggests that e-Government (electronic government) is a system of government that adopts Internet-based technology, in order to complement and improve governmental program and service system. The main objective is to provide the best service and maximum satisfaction to the service user, i.e. the people and stakeholders. The same thing was stated by Rahman et.al. (Rahman, Low, Almunawar, Mohiddin, & Ang, 2012) who suggest that, in the narrow sense, e-Government can be defined as the use of information and communication technology, especially the Internet and Web technology in carrying out government activities in relation to government's stakeholders.

World Bank (World Bank, 2001) sees that e-Government is a part or the adaptation of banking technology which constantly develops around the world. The development of e-Government is intended to improve efficiency, effectiveness, transparency, and accountability of government management by using internet media and other digital technologies. Indrajit (Richardus Eko Indrajit, 2013) added that e-Government is an effort to create an atmosphere of government administration that is in accordance with the common goals of a number of interest groups.

e-Government is a governance based on information technology to improve the performance of the government, especially in relation to society and the private sector, as well as other interest groups in order to achieve good governance. e-Government program can be used in: (a) the government's use of technology, especially technology that utilizes web-based internet applications in order to improve access to governmental service by the people, private sectors, employees and other government's stakeholders; (b) a reform in the ways and performance of the government, various information and service to internal and external clients so that they can provide benefits to the government, the community, and private sector; (c) the use of information technology such as wide area network (WAN), the internet, the world wide web, and computers by government agencies to reach out to the people, private sectors and other government branches, improve services to the public, private sector, industrial sector and empower the people through access to knowledge and information, as well as making the government performs more efficiently and effectively.

e-Government is the result of government efforts to reach out and provide better services to the people. With openness and transparency inherent in the system of e-Government, due to the principles of the Internet, e-Government brings the government closer to its citizens. Therefore, e-Government has a larger social dimension, because e-Government will encourage a more comprehensive and representative democracy. In terms of economic knowledge, competitive advantage depends on the ability to adapt to environmental changes due to the continuous generation and application of new knowledge. Kumar (Kumar, 2015) emphasized that many businesses currently cannot even function without using Information and Communication Technology (ICT) in their operations. Thus, the use of ICT is very significant in order to face increasingly fierce global competition.

Based on the various literatures above, e-Government can be defined as the utilization of information and communication technology in order to achieve the following objectives: (1) improving government's efficiency; (2) improving and optimizing public services; (3) sharply increasing public's access to information; and (4) creating a transparent and accountable government.

Cyber Security and Cyber Threat

Even though e-Government can be regarded as a solution in administration system by enabling better services and more transparent government, the use of Internet technology in administration system as well as a variety of other public services will also allow it to be vulnerable to threats inherent in the use of cyber technology within e-Government system.

Forrest Hare (Hare, 2010) in his article entitled "The Cyber Threat to National Security: Why Can't We Agree?" argues that the threats present in cyberspace are very broad and unique. It is broad in the sense that the threat agent that can carry the threats could come from states, criminals, hackers, or terrorists. In addition, the type and target of the threat is also quite diverse.

Hare mentioned that every state has different vulnerability in regard to cyber threat. This vulnerability is strongly influenced by the characteristics of each state. A threat to one state is not necessarily a threat to other states. Richard Clarke(Clarke & Knake, 2010), former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism of USA, in his book entitled *Cyber War*, defines cyber war as an act of penetration by a state against other computer networks with the aim of causing damage and interference.

Barnum stated that

> "the traditional approach to cyber security which focuses on understanding and handling threats, weakness and configurations is needed but will be insufficient in dealing with cyber security." Barnum suggested the need for centrality in "understanding the behavior, abilities and intentions of the enemy," in anticipation of current and future cyber-attacks.

In the British defense doctrine of "ability + intent = threat," intelligence is very important in the threat-centric approach of cyber security. However, in the context of cyberspace, "opportunities" is the third factor that can increase or reduce the sophistication level and the broad spectrum of threats that take advantage of these opportunities. By considering these various factors, in the context of threats to banks and the payment system, including the government system, it becomes clear that the threat of cyber-attacks will also be increasing (Craig Rice et.al., 2013). The relatively low impact is that the high probability of cyber-crime has been limited to tolerable friction or points.

Furthermore, Soewardi(Bagus Soewardi, 2013) mentioned that cyber world can also be used as a political tool through the spread of false news for the purpose of political provocation and economic engineering. Internet social engineering attacks and public and international opinion making on certain topic, either in the form of propaganda or agitation campaigns, are now also widespread throughout the internet. These interest groups can easily do so without having to spend as much money and resources as they did in the past. Therefore, a rule or law is needed as a fence to protect and maintain security in cyberspace to anticipate and overcome various threats that can arise or be born from the invention of information technology and telecommunications.

Cyber law is a law that regulates the intangible actions that occur in the digital world such as by giving legal status to intangible information in cyberspace, security and privacy of that information and crimes related to damage caused by virtual information etc. Cyber law is very

important for managing various problems in the cyber domain. Security is especially important in maintaining the Information and Communication Technology (ICT) assets of each organization. These assets can be internal or external, such as data, information, knowledge sources, programs, hardware, network and so on. Threats to the security of ICT systems can come from many sources and in various forms.

In general, internal threat to the security of ICT systems in e-Government may come from the private or public agency personnel, customer or the end user of the e-Government program. While external threats to the security of e-Government program generally comes from hackers, criminal groups or terrorist organizations and intelligence & investigation agencies. Threats to assets can also vary greatly in type and intensity, as well as the impact values of the threat.

Potential and currently existing threats in cyber security are the most serious challenges of the 21st century. The threat arises from various sources, and manifests itself in activities that interfere with and targeting individuals, businesses, various national infrastructures and the government. The effects they pose carry a very significant risk to public safety, state security and the global stability of international community as a whole. However, although the risks posed by the abuse of ICT are very significant for public safety, state security and the stability of international community, the abuse of information and communication technology can be easily hidden.

The Identity and origins of the perpetrators or their motive in causing the disorder can be easily disguised – hence it is difficult to know the true identity and motive of the perpetrator. Often, the identity and motives of the perpetrators of these activities can only be estimated based on their target, impact or other indirect evidence. Perpetrators of threat can operate with substantial immunity because virtually they can come from anywhere. Their motives also vary greatly, ranging from just wanting to show technical abilities, stealing money or information, to as an extension of state conflict. Many of the dangerous tools and methodologies related to the use of information and communication technology originated from the attempts of criminals and hackers in the cyberspace. The sophistication and scale of criminal activity that continues to increase also contributes in increasing the potential for various dangerous actions in the cyber domain.

The abuse of ICT in cyberspace in creating such threats can be said to be ideal for those who carry out attacks such as hackers and other criminals who use cyberspace for their interests, but are not very ideal or can be very difficult for those in defensive positions such as government and related stakeholders, who are bound by the applicable legal corridors. This condition of asymmetric warfare is illustrated very clearly by Buffaloe (Buffaloe, 2006) through the equation of asymmetric warfare as shown in the following figure.

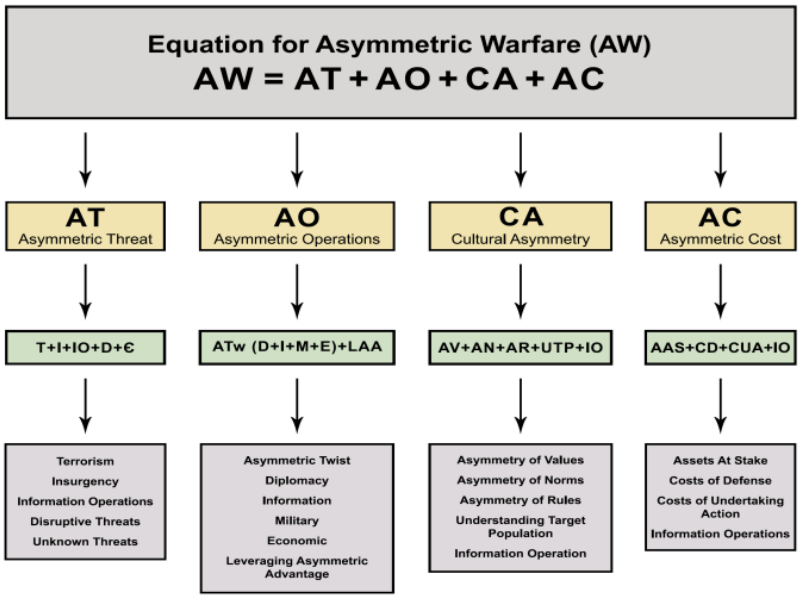

Figure 1. Equation of Asymmetric Warfare
Source: Buffaloe, 2006

In the perspective of asymmetric warfare, the use of cyberspace as a medium in creating threats is something that is ideal that meets the entire basic conditions of asymmetrical warfare. With relatively low operational costs (AC), it is capable of causing a very wide threat (AT), which is difficult to predict, detect, anticipate, and allows the perpetrator to remain anonymous (AO) (Pino, 2011), and is impossible to avoid due to the world being very dependent to the benefits of cyberspace in ICT (CA). In line with Barnum, Buffaloe further argues that the center of gravity and determinant of victory in asymmetric warfare as a population-centric non-traditional warfare or a population-centered nonconventional war strategy is located in society as the center of gravity or determinant of victory in war. Hence, it also applies in the threat management related to the abuse of ICT in cyberspace.

e-Government management means coherently managing a large portfolio that includes a variety of different responsibilities with all subjects who use the e-Government facilities, so that every user in the e-Government system can be recognized. The following is schematic representation of the explicit classification of e-Government community and applications – the government, citizens, workers and private sectors are interrelated in some activities. Most e-Government activities are targeted to Citizens, both directly and indirectly, which is one of the interconnections in e-Government. All communities and activities of e-Government are interlinked as shown in the following figure.

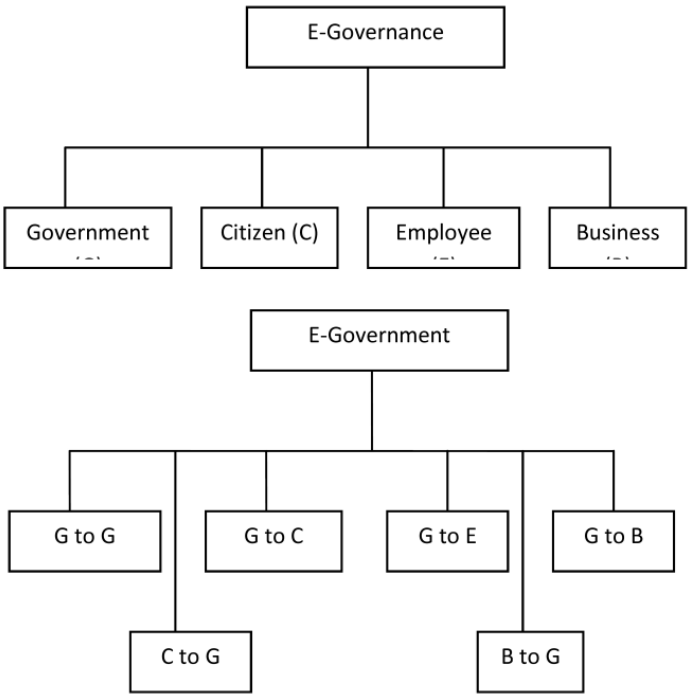

Figure 2. Relationship Scheme in e-Government
Source: Kumar, 2015

The illustration above provides an overview of a layered approach related to the integration of e-Government services and illustrates the importance of a legal reform in the cyber sector. As shown above, transformation involves 4 communities and 6 results in all four communities. The main objective is to get an e-Government with sustainable development capacity on all fronts.

Globally there are a variety of models or ways to implement e- Government in each of these sectors. The illustration above shows the existence of a community and different results related to the usefulness and credibility of the tools being used. Cyber security is an activity to protect information and information systems (networks, computers, databases, data centers and applications) using appropriate security procedures and technologies.

Thus, cyber security in general can be interpreted as covering all protection activities in the cyber domain. While cyber defense is related to activities that are far more specifically related to certain aspects and organizations. The differentiating factor between cyber security and cyber defense in the cyber realm lies in the nature of its activity rather than the threat that it handles, assets that it must protect and the applied mechanism to ensure the protection in the cyber realm. Cyber defense is related to defensive actions against activities, especially those originating from actors belonging to the category of threats who have political motivation, quasi-political economy motivation that has an impact on national security, the public and community welfare.

Environmental cyber defense requires technological capabilities in order to provide real-time protection and incident response at all times. This is needed to pave the way for interoperability and the creation of ICT systems that are in line with the e-Government program. Partnerships between the public and private sectors are key components of cyber security in e-Government. The partnership can easily face coordination problems. They can also significantly increase information exchange and cooperation. Public and private involvement will take various forms which will later shape resilience in cyberspace such as cyber awareness, various training and improvements to cyber technology, vulnerability improvements

and cyber recovery operations. This action will be very helpful in improving technological development and cyber capabilities in the public sector.

Participation of community and other government's stakeholder in facing the cyber-threat is indispensible in achieving the main objective of e-Government program, namely the creation of sustainable development in all fronts. By understanding the e-Government strategy of Brunei Darussalam which places the cyber domain as the spearhead of its non-military defense, the Government of Indonesia and the people of Indonesia can learn precious lessons in building a better e-Government system for Indonesia. After all, e-Government is a government administration system that has become a critical communication center of the world today that greatly determines the progress of a state – Indonesia is no exception.

RESULTS

General Description of Research Subjects and Objects

The Ministry of Foreign Affairs and Trade (MOFAT) was formally established after the full independence of Brunei Darussalam on 1 January 1984. On 1 August 2005, the Department of Trade and Department of International Relations of Ministry of Industries and Primary Resources were merged into the Ministry of Foreign Affairs to become the Ministry of Foreign Affairs and Trade (MOFAT).

The Ministry is responsible for handling Brunei Darussalam's foreign affairs, managing international diplomatic missions and foreign trade policy. The Ministry is headed by the Chief Minister and the Second Minister for Foreign Affairs and Trade; with Sultan Hassanal Bolkiah as the Chief Minister.

IT Protective Security Services (ITPSS) was established in 2003 as a local pioneer in the field of information security solutions, which provides a variety of specialized information security services and physical security services including penetration testing, digital and mobile forensics including data recovery, managed security services (MSS), cyber and Info-sec awareness trainings, physical and electronic securities including secure event management.

As a pioneer in the field of information security solutions and services in Brunei Darussalam, ITPSS is consisted of a team of experts in Information and Cyber security as well as an experienced management team that is consistently certified with the highest security qualifications by renowned professional certification bodies such as SANS Institute, EC-Council, CompTIA, AXELOS (Prince2, ITIL) and vendor-specific qualifications from Microsoft, Oracle, Cisco and Jintan Saru.

In addition to having more than 10 years of experience in handling leading projects for both private institutions and Government agencies in Brunei Darussalam, ITPSS is also responsible for conducting Incident Response and Handling through its role as Brunei Computer Emergency Response Team (BruCERT). Formed in 2004, BruCERT is Brunei Darussalam's trusted referral agency in handling online threats and computer security incidents in Brunei Darussalam.

BruCERT has continued to raise public awareness about cyber security and cyber safety through outreach programs that include giving lectures to students, roadshows, booklets, radio shows, newspaper advertisements, television commercials & cinemas advertisement.

Prime Minister Office (PMO) of Brunei Darussalam was established on 1 January 1984 at the full independence and sovereignty of Brunei Darussalam. At present there are 21 departments under the scope of the Prime Minister Office of Brunei Darussalam. This office is led by Sultan Hassanal Bolkiah of Brunei Darussalam as the Prime Minister. The Prime Minister's Office is the central coordinating body for all Ministries and

Government Agencies relating to Brunei Darussalam's national policies and also the central institutions in the management and administration of the Government and Civil Service of Brunei Darussalam.

Brunei Darussalam's e-Government Strategy

Brunei Darussalam's strategic plan or framework for e-Government was first launched in 2001, and reviewed in 2005. Based on a review in 2005, the government of Brunei found that the program should put more emphasis on citizen-centric service delivery where the government must focus more on a service system that focuses on the community or population. The e-Government initiative was a key program for the development of Brunei Darussalam Information and Communication Technology (ICT). In e-Government Strategic Plans of Brunei Darussalam 2005-2009, in addition to the establishment of the Brunei Information Technology (BIT) Council, the emphasis on citizen-centric service was followed up not only by building websites for community services, but also with increasing services for private sectors. Thus, citizen-centric service are the main principle in Brunei Darussalam's e-Government development.

In line with the increasing dependence to ICT, citizen-centric service is the key to change not only the government service system by the state apparatus in Brunei, but also the entire people of Brunei Darussalam. In addition, a Change Management Team has also been formed to learn ways and strategies to bring about changes in the organizational culture of business processes to move in the desired direction both in terms of habit patterns and mindset than the overall state apparatus.

The success of the Brunei Darussalam e-Government program is largely determined by the existence of a positive interaction among all stakeholders in Brunei Darussalam, both from the Brunei's governmental apparatus, the industrial sector, and the people of Brunei Darussalam themselves. The contribution and input to the e-Government program of Brunei Darussalam is a shared responsibility for all stakeholders in Brunei Darussalam. Therefore, all stakeholders in Brunei Darussalam have an obligation to adopt a forward-looking and problem-solving mindset in order to achieve a common goal, namely to produce the best service system for the entire Brunei community. To achieve this, concrete and proactive actions need to be taken to increase the capacity to develop human resources in the ICT field.

In that context, the Prime Minister Office, and the Ministry of Communication play leading roles in community and industrial services, which are then followed by active participation and commitment from company leaders and those engaged in the industrial sector, as well as their representatives and other stakeholders in the public sector.

Strategic Priorities for E-Government Development in Brunei Darussalam

The Government of Brunei Darussalam in 2009-2014 set 5 strategic priorities to realize the development of e-Government in Brunei Darussalam. By focusing on development programs, e-Government was emphasized on how to increase resources to strengthen ICT facilities and encourage government agencies to be able to collaborate and accelerate integration, accessibility and efficiency of e-Government services including the development of ICT capabilities (Government of Brunei Darussalam, 2009).

The strategic priorities and objectives of the development include:

1. Capacity Building and Cyber-Capacity. The aim is to provide government apparatus with ICT skills, provide career opportunities that are able to attract and accommodate professionals in the ICT sector in public sector, as well as building competencies and guides for professionals in the ICT field.

2. Improve Government Services. The aim is to improve government ICT service policies and management processes to ensure that the government can achieve e-Government goals effectively and efficiently, through an open and accountable framework.
3. Strengthening Security and Trust in the Cyberspace. The aim is to ensure that all of the government's ICT facilities, systems and applications are in a safe, protected and guaranteed by the best level of security.
4. Integration of Government. The aim is to establish and enhance the coordination capabilities of government agencies in building an integrated e-Government service.
5. Building Integrated, Accessible and Satisfying E-Government Services. The aim is to build and produce online services for the community that are efficient, safe, and easily accessed and used.

With a focus on citizen-centric services system, these strategic priorities are then translated into work programs as shown in the following figure.The aim of the work program is to ensure that both the center and specific agencies work in line with the vision and mission of the e-Government that has been planned. The programs themselves will also carry out a list of projects that must be carried out and will be monitored effectively and sustainably.

Brunei Darussalam's Digital Government Strategy

The Digital government Strategy 2015-2020 is directed towards supporting the vision of Brunei Insights 2035. The approach taken by Brunei Darussalam in its digital government strategy is to apply the Whole-of-Government principle towards innovation and service provision, which drives the government's digital transformation to create a service that is

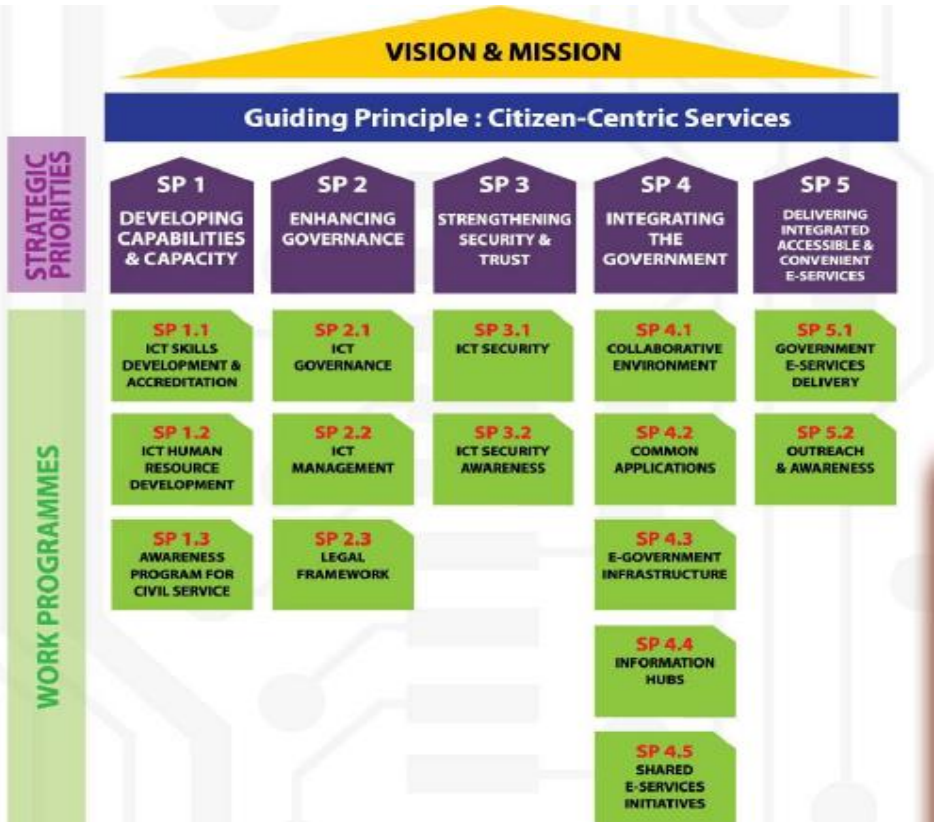

Figure 3. Key Strategic Priorities for the Development of e-Government in Brunei Darussalam
Source: Government of Brunei Darussalam. 2009

simpler, faster and more accessible. The Government of Brunei Darussalam aims to create an easy-to-use service to encourage public agencies to reengineer their efforts to fully utilize ICTs to optimize their processes and performance by taking into account the need for increased cooperation in various business entities or public. This encourages the public, government, and stakeholders in Brunei to foster a mindset that is forward thinking that may help in increasing the speed of adoption and ICT capability of government officials in Brunei Darussalam.

Brunei Darussalam's Digital Government Strategy also provides an opportunity to review existing infrastructure and systems. Brunei Darussalam ensures that these infrastructure and systems remain and can be used effectively to maximize their capacity. In addition, data and information is a very important foundation in the decision making process. Therefore, Brunei Darussalam continues to develop their capabilities and technology, so that government-owned data can be used to produce a valuable view so that the Government of Brunei Darussalam is able to make a decision based on accurate information.

The success of Brunei Darussalam's digital government strategy is largely determined by the active participation of all stakeholders in Brunei Darussalam to adopt and adjust their mindset to achieve the goals of the Digital Government. In this context, the active participation of all government agencies, and of course followed by active participation and commitment, from CEOs, company leaders, and those engaged in the industrial sector, as well as representatives, and other stakeholders in the public sector, play an important role for the success of e-Government.

In order to successfully realize digital government strategy (e-government), the Government of Brunei Darussalam has set six areas of focus in their e-Government development:

1. Service Innovation. With an increasingly sophisticated and dynamic society, government agencies must develop new ways and innovations in providing services to the community and private sector with better transparency and accountability.
2. Collaboration and Integration. Government agencies are required to work together to face an increasingly complex environment. This requires a Whole-of-Government approach to improve collaboration and integration of government processes.
3. Capability and Mindset. People will always remain a key factor that will lead to the successful application of any technology. It is important to encourage forward-thinking mindsets and collaborative cultures. This will increase the speed of the adoption of the new system, the level of utilization of the system and the ability of government officials.
4. Optimization. To offset the rapid development of technology, the government has implemented various IT systems and platforms. Thus, the Government needs to optimize the use of digital assets to guarantee the effectiveness & optimization of results.
5. Security. Following the previous 2009-2014 strategic plan, security will remain the main focus. The Government of Brunei needs to maintain situational awareness of its digital assets and environment at all times. Adequate action will be taken to minimize risk and increase the ability to effectively respond to cyber incidents.
6. Management of Company Information. With an economy that is driven by current knowledge, information is the main foundation that is very important in advancing a

nation. It is very important for the government to manage explosive data growth by compiling, describing and managing information assets which can then be used to produce a view that will assist in the decision making process.

Based on the 6 focus areas in the development of digital government above, the Government of Brunei Darussalam established six programs to achieve the 2015-2020 Digital Government Strategy:

1. Advancing Digital Services. Service is the main vehicle in which the Government can provide value to stakeholders and facilitate the desired results. This program aims to make service interactions between the Government and stakeholders to be easier, friendlier, more transparent and effective. The output is that main services can be accessed anytime, e.g. collecting government revenues digitally.
2. Implement Universal Access in the Government System. Identity is a concept and mechanism that captures the uniqueness and attributes of a particular entity. Having a unique and universal identity for every citizen and business makes it easy for them to access Government services. This universally accepted identity also allows the Government to obtain a holistic view of citizens and business, which enables the Government to better anticipate their needs. The output is One ID for citizens, One ID for businesses, Services that support One ID.
3. Strengthening Security. This program will develop and implement the National Cyber Security Framework to address and overcome cyber threats and provide a robust and reliable digital platform that maximizes the full potential of the use of digital space (cyberspace). The output is an integrated approach by all sectors to national cyber-security.
4. Increasing the involvement of Stakeholders. The program is focused on building platforms and implementing measures to improve two-way communication between the government and stakeholders, with the aim of improving government services, assisting in formulating new initiatives and also handling public issues. The output is a new platform for stakeholder engagement and a regulatory framework for managing stakeholder engagement.
5. Optimization of Digital Assets. This program is intended to ensure that all ICT investments are fully utilized, and the realization of the expected return on investment. To ensure the efficiency of government activities, it is very important to continue to assess whether digital assets have been fully utilized and managed to meet established objectives. The program also aims to review the utilization of the existing system and take appropriate actions. The output is maximizing the value of existing digital assets.
6. Developing Management Information Capability. This program focuses on the processes, equipment and the ability to coordinate and manage data that are created, stored, used and processed by the government. The amount of data being generated grows at an exponential rate. The government will be able to better understand the state of the company's business processes, and the effectiveness of decisions and actions made by the company through better management of the data and information cycle. The output is the realization of Company Information

Management processes, tools and capabilities.

The strategic objectives to be achieved by the Brunei government as set forth in the Brunei National ICT White Paper 2016-2020 are:

1. A developed economy driven by the ICT sector.
2. ICT-Smart Citizens.
3. A Connected and Efficient Nation.

The projections and also the development of their human resources in the field of ICT in order to realize the strategic goals of ICT-Smart Citizens are set forth more specifically in National ICT Manpower Masterplan for Brunei Darussalam whose strategic goal is to grow the number of skilled ICT professionals to 6,000 from 4,200 ICT professionals who exists now by creating 1,800 additional jobs in the ICT field by 2020 (Ministry of Communication Brunei Darussalam, 2016a).

The Key enablers are the key factor in supporting the successful implementation of the Digital Government Strategy of Brunei Darussalam as stated in the Brunei National ICT White Paper 2016-2020 which includes:

1. Arranging data center hubs to facilitate information access, data sharing and analysis;
2. Creating an important ICT policy to guide the overall development and management of IT;
3. Provide adequate attention to ICT security for risk management;
4. Seek the development of labor as a key aspect for resource management;
5. Ensure that infrastructure support is performing well, available and easily accessible.

Development of Cyber Security and Cyber Safety in Brunei Darussalam

The Brunei National Agency in charge of IT securities is ITPSS (IT Protective Security Services) which is tasked to accommodate information or physical security solutions incorporated in information technology to avoid information theft.

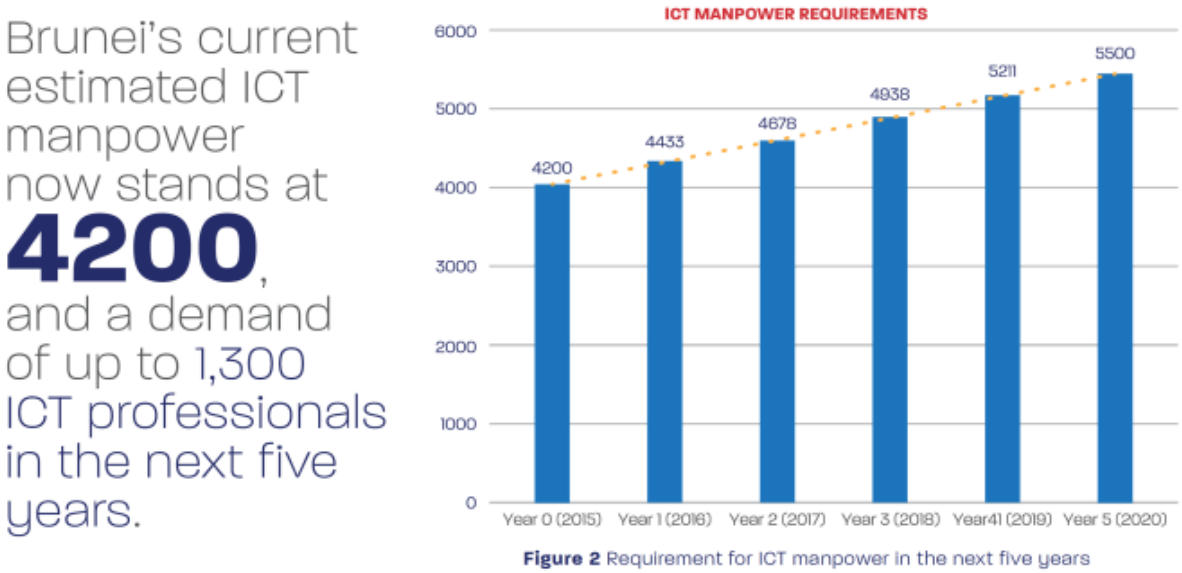

Figure 4. National ICT Manpower Masterplan for Brunei Darussalam
Source: Ministry of Communication Brunei Darussalam. 2016

There is a separate team called BruCERT in ITPSS which acts as a response team and in charge of immediate handling of incidents related to IT in Brunei. In addition, BruCERT also has a role and function in raising public of IT security through education, workshops and seminars.

The Brunei Ministry of Education includes cyber security awareness into their education curriculum. In the third year, there is a syllabus about the risks, hazards, and internet etiquette as well as email security. BruCERT has been implementing the Cyber Civil Servants awareness training program and the Awareness Outreach Program for school since 2005. They also carry out dissemination of information through printed and digital media and roadshows to raise the awareness of youth and community members in Brunei related to cyberspace. All of them are integrated in a joint policy called the Brunei Insight 2035.

Brunei Computer Emergency Response Team (BruCERT) was formed in May 2004 in collaboration with the Ministry of Communication. The team coordinates with local and international computer emergency response teams, business agencies, government agencies and Internet service providers. Authority for Info-Communication Industrial Technology is a state telecommunication and radio frequency regulator, and is responsible for information infrastructure development. The government focuses on implementing cyber defensive capabilities, protecting internal systems and improving the development of information technology. Although the Ministry of Defense is not an institution responsible for cyber security, the Brunei military is committed to using information technology and computers to increase its diplomatic and defense capabilities.

With the progressive adoption of ICT in Brunei Darussalam, one of the main concerns of the Brunei Darussalam government is to pay special attention to the security of Information Technology and Communities in Brunei Darussalam. Increasing the use of ICTs automatically increases the need to protect information and data, computing devices, networks and the services they provide from cyber threats that are developing in the cyber domain. As a major milestone in the field of ICT security, the government of Brunei Darussalam has made significant progress by carrying out several key initiatives (Ministry of Communication Brunei Darussalam, 2016b), including:

1. Implementing Regulations for Computer Abuse in June 2000,which is an order to make provisions to secure computer material from unauthorized access or modification and various related matters;
2. The establishment of Brunei National Computer Emergency Response Team (BruCERT) in May 2004. The first trusted one-stop referral body in the state was established to deal with security incidents related to computers and the internet in Brunei Darussalam. BruCERT is also coordinating with local and international CSIRTs, network service providers, security vendors, government agencies, and other related organizations to facilitate the detection, analysis and prevention of security incidents on the Internet;
3. Internet Ethics and Cyber Security Vigilance Program. Starting in 2009, the program held seminars targeted at students, teachers, and parents of students in local educational institutions;
4. Development of National Cyber Security Framework called e-Government National Center (EGNC) under the Prime Minister Office (PMO). Since 2014, it has developed a National Cyber Security Framework to provide a comprehensive framework for managing cyber security at the national level. These efforts are shown in the following figure.

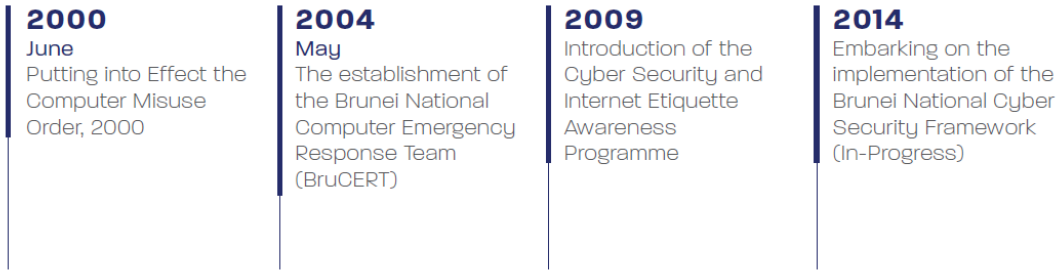

Figure 5. Brunei's National Security Journey
Source: Ministry of Communication Brunei Darussalam. 2016

DISCUSSION

Based on the explanation above, it can be seen that the key to Brunei Darussalam's e-Government strategy in overcoming cyber threats lies in the focus and understanding that the program should be emphasized on citizen-centric service delivery, or a service system focused on the people or community. This is in line with what was stated by Buffaloe who argues that the center of gravity in asymmetric warfare as a population-centric nontraditional warfare is the society or the people who will be the determining factor of victory.

The existence of cyberspace as a new war mandala must be dealt with by all states in the world, including Brunei. Thus, by placing the principle of citizen-centric service delivery as the key to their e-Government strategy, it can be seen that the Brunei Darussalam government fully understands the form and nature of asymmetric cyber threats that cannot be addressed without the active participation of all components of the state of Brunei Darussalam. Cyber development around the world that leads to the Internet of Things (IoT) is so rapid that it is largely driven by market needs for everyday products such as smartphones, and various electronic equipment and equipment that have IP-address sensors that can be activated. On the one hand, it can provide opportunities and benefits because the data that can be collected, contextualized and then analyzed in accordance with the insight that will be made, as shown in the field of health and sports. However, these opportunities can also turn into threats if not managed carefully, given the wide range of threats and threat agents in cyberspace as suggested by Forrest Hare.

In regard to this, the Brunei government sees it as an opportunity without dismissing the threat that might arise from the growing development of IoT. This can be seen from the strategic targets they are targeting in their ICT White Paper, which requires the realization of ICT-Smart Citizens in addition to the target of advanced economies driven by their ICT sector. The Brunei government sees that the use of IoT as an opportunity can be applied in the energy sector to monitor its extensive equipment network in the face of cyber-attacks through smart asset management, as well as the transportation sector in order to face an increasingly complex transportation landscape, which of course must also be balanced with the development of their cyber capacities and capabilities to anticipate possible threats.

Capacity building and cyber capabilities in Brunei Darussalam is implemented by adhering to the strategic objectives of ICT-Smart Citizens which is the key to realize better cyber resilience for Brunei. Referring to the 2016-2020 Brunei National ICT White Paper, it can be seen that the population-centric nature of Brunei Darussalam's e-Government development is very thick. This can be seen in Key Enablers which they set as a key factor in supporting the success of their Digital Government Strategy which also projects the development of their human resources in the field of ICT to support their economy in the future in addition to infrastructure

development and ICT management that supports their cyber vigilance.

The development of human resource capacity and capability in the field of ICT as well as awareness of cyber threats has been carried out and instilled by the Brunei government early through the Ministry of Education with their Internet Ethics and Cyber Security Awareness Programs, which also involve the participation of all Brunei people (not only students, but also teachers and parents of students) through local educational institutions.

This is then supported by a strong legal foundation on Computer Abuse Provisions in 2000 to secure computer material from unauthorized access or modification and various other related matters that could potentially cause cyber threats. As such, the Government of Brunei has at least closed various gaps that might cause cyber threats. So, when there is an attack that uses cyberspace as a medium for Internet social engineering attacks in order to form public opinion that can harm and threaten Brunei Darussalam's public security, the Brunei government can immediately narrow the threat scope and potential threat agent of the intended attack, as stated by Forrest Hare.

The population-centric nature of Brunei Darussalam's e-Government strategy in dealing with the cyber threats mentioned above, if examined further can also support Brunei Darussalam's national resilience in other fields outside the cyber field. By including community participation in e-Government strategies through the programs of "One ID for citizens, One ID for businesses, and Services that supports One ID," the Government of Brunei can also indirectly mitigate other threats outside of cyberspace through the participation of Brunei community in the program. This is possible because the space and opportunity that could endanger the security and safety of the state can be limited and monitored digitally through Brunei Darussalam's e-Government strategy

CONCLUSION

Brunei Darussalam's e-Government strategy in overcoming cyber-threats is implemented in stages, i.e. starting in June 2000 with the establishment of rule of law regarding the computer abuse in 2000, followed by the establishment of Brunei Computer Emergency Response Team (BruCERT) in May 2004, the introduction of Internet Ethics Awareness and Cyber Security Program in 2009, and the Development of National Cyber Security Framework in 2014. The whole thing is integrated in a joint policy called the Brunei Insight 2035.

Brunei Darussalam's e-Government strategy in overcoming cyber threats is carried out by focusing on citizen-centric service delivery. This is in line with David Boffaloe's basic principle of asymmetric warfare, namely a population-centric non-traditional warfare where its center of gravity that determines victory lies in the people.

The stage begins with the formation of cyber ethics among the people by enacting rules governing the ethics and how to use ICT responsibly which becomes the foundation for Brunei's national cyber awareness and vigilance. This was then continued with the development of cyber security, as well as the capacity and capability of Brunei's cyber community, which was followed by the development of a national cyber security framework with the final stage towards the Brunei Insight 2035 which put the cyberspace as the spearhead of Brunei Darussalam's national military defense and development.

RECOMMENDATION

e-Government strategy is a government administrative system that has become the center of information and communication services which is very vital in the world today and is crucial for the progress of a state. The development of ICT that has evolved towards the use of ICT and also the massive development of IoT has encouraged all states in the world to to adjust to the development.

In reflection of Brunei Darussalam's strategies to overcome cyber threats which manage to synergize security services and national economy development, Indonesia can learn precious lessons in building its national resilience. By utilizing the citizen-centric service delivery approach as applied by the Brunei government in building e-Government, Indonesia can develop Indonesia's national resilience, not only in cyberspace but also by synergizing it with other defense and security outside of the cyber domain as explained previously.

REFERENCES

Bagus Soewardi. (2013). *Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia*. Media Informasi Ditjen Pothan Menhan.

Buffaloe, D. L. (2006). Defining Asymmetric Warfare. *The Land Warfare Papers*.

Clarke, R., & Knake, R. K. (2010). *Cyber War: The Next Threat to National Security and What To Do About It*. *Terrorism and Political Violence*. https://doi.org/10.1080/09546553.2011.533082

Craig Rice et.al. (2013). *Cyber Threat Intelligence An analysis of an intelligence led, threat centric, approach to Cyber Security Strategy within the UK Banking and Payment Services sector* (Cyber Threat Intelligence Research Paper). United Kingdom.

Government of Brunei Darussalam. (2009). *The E-Government Strategic Plan 2009-2014*. Brunei Darussalam.

Government of Brunei Darussalam. (2015). *Digital Government Strategy 2015 – 2020*. Brunei Darussalam.

Hare, F. (2010). The Cyber Threat to National Security Why Can't We Agree. In *Conference on Cyber Conflict Proceedings*.

Kumar, P. (2015). A Case Study on Cyber Security in E-Governance. *International Research Journal of Engineering and Technology (IRJET)*.

Ministry of Communication Brunei Darussalam. (2016a). *National ICT Manpower Masterplan for Brunei Darussalam*. Brunei Darussalam.

Ministry of Communication Brunei Darussalam. (2016b). *National ICT White Paper for Brunei Darussalam: National Digital Strategy 2016-2020*. Brunei Darussalam.

Moleong, L. J. P. D. M. A. (2017). Metodologi Penelitian Kualitatif (Edisi Revisi). In *PT. Remaja Rosda Karya*. https://doi.org/10.1039/b709107a

Mustopadidjaya, A. (2003). *Sistem Administrasi Negara Kesatuan Republik Indonesia*. Jakarta: (SANKRI), LAN.

Pino, M. (2011). *Cyber Threats to National Security; Symposium Five: Keeping the Nation's Industrial Base Safe from Cyber Threats*.

Rahman, M. H., Low, P. K. C., Almunawar, M. N., Mohiddin, F., & Ang, S.-L. (2012). *E-Government policy implementation in Brunei: Lessons learnt from Singapore*. *Active Citizen Participation in E-Government: A Global Perspective*. https://doi.org/10.4018/978-1-4666-0116-1.ch018

Richardus Eko Indrajit. (2013). Seri 999 E-Artikel Sistem Dan Teknologi Informasi.

Sugiyono. (2016). Memahami Penelitian Kualitatif. *Bandung: Alfabeta*. https://doi.org/10.1111/j.1365-2036.2009.03946.x

World Bank. (2001). *Issue Note: E-Government and the World Bank*.