Towards Data Sovereignty in Cyberspace

Yudhistira Nugraha
CDT in Cyber Security
University of Oxford
yudhistira.nugraha@cs.ox.ac.uk

Kautsarina
Research and HR Development Agency
Ministry of ICT, Indonesia
kautsarina@kominfo.go.id

Ashwin Sasongko Sastrosubroto
Research Center for ICT
Indonesian Institutes of Science
ashwin.sasongko.s@lipi.go.id

***Abstract*—From a national security perspective, cyberspace is a shared domain which requires a shared responsibility between stakeholders at national and global level. Many countries have taken concrete steps to safeguard and protect their sensitive national data in cyberspace against cyber threat such as foreign intelligence services. Data sovereignty is of paramount importance to a nation-state such as Indonesia against the domination of foreign Internet service providers. Data sovereignty requirements can be viewed as reasonable efforts by nation-states to subject national sensitive data flows to and across national borders. Such data sovereignty requirements aim to safeguard and protect basic interests of nation-states in relation to data confidentiality, data integrity, and data availability. This study examines the Indonesian Government's requirements for data sovereignty and proposes initial technical proposals for data sovereignty requirements such as an encryption, national email services, data center localisation, national routing of Internet traffic, and national backbone communications infrastructure. As a new domain, we believe that data sovereignty raises many questions for related future research.**

***Index Terms*—Cyberspace; data sovereignty, data security, requirements, Indonesia.**

I. Introduction

As stated in the preamble of the 1945 constitution of the Republic of Indonesia, Indonesia's national aspirations aim to protect the whole people of Indonesia and the entire homeland of Indonesia; to advance general prosperity; to develop the nation's intellectual life; and to contribute to the implementation of a world order. In addition, these objectives are supported by the Act No. 3/2002 on state defence, which aims to protect state sovereignty, national territory, and the nation's safety against all types of threats [18].

On the other hand, in response to reported secret intelligence collection by the Australian Signals Directorate (ASD), the Guardian Newspaper revealed that the ASD intercepted communications from the mobile phones of top Indonesian officials include President Susilo Bambang Yudhoyono, the Vice President, the First Lady and several cabinet ministers [20]. Such global communications surveillance is widely operated by the "Five Eyes" (the U.S., the U.K., Canada, Australia, New Zealand) intelligence alli. It is clear that sensitive information about Indonesia might have been distributed among the five countries because of the vulnerability of information and communications technology (ICT) infrastructure and services in Indonesia. Thus, information security should be considered as an important factor in the ICT governance.

Several recent attempts have been proposed by other countries such as Brazil, Germany, China, and Russia to better regulate their data sovereignty requirements against the domination of the US communications infrastructure and services. [2] [4] [5] [7] [10] [11] [22] . These technical proposals are national email, localised routing of Internet traffic, undersea fiber optic cable and localised data centre. However, Maurer et al. in [15] assessed that those proposal are unlikely to protect against the global communications surveillance by foreign intelligence services. They pointed out that encryption mechanisms are feasible solutions for securing sensitive data against foreign surveillance [15].

A number of studies have been conducted to improve the policy and requirements on Cyber Security in Indonesia. Nugraha et al. in [19] reveal that the Cyber Security readiness in Indonesia is at a low level compared to the five pillars of the Global Cybersecurity Agenda (GCA)'s ITU Framework. Thus, special attention is highly necessary to improve national Cyber Security. Moreover, Nugraha et al. in [18] consider the Indonesian Government's requirements for state self-defence in response to reported secret intelligence collection by the Australian Signals Directorate (ASD). Strong regulations and requirements are of paramount importance to protect and safeguard our national interests.

From Indonesian policy makers' perspective, the term "data sovereignty" is not yet in use, but it refers to the national legislation on the state defence against external threats such as state-actors and non-state actors. Indonesian law number 11/2008 on Electronic Information and Transaction and its related Government Regulation on Electronic System and Transaction Operation number 82/2012 stated that all institutions providing public services shall store their data within the country. However, the definition of public services by the law number 25/2009 on public services is defined broadly and is vague. In this paper, data sovereignty refers to the reasonable effort by nation states to subject information flows to national jurisdictions [22]. Polatin-Reuben et al. in [22] point out two poles of data sovereignty, which are (1) weak data sovereignty that allows "private sector-led data protection initiatives with an emphasis on the digital rights aspects of data sovereignty"; (2) strong data sovereignty that favours "a state-led approach with an emphasis on safeguarding national security". Moreover, Peterson et al. in [21] define data sovereignty as an attempt at "establishing data location at a granularity sufficient for placing it within the borders of a particular nation-state".

Thus, this study investigates the Indonesian Government's requirements for data sovereignty and proposes an initial set of technical requirements for data sovereignty and its limitations.

The remainder of this article is structured as follow: Section 2 describes approaches to illuminate potential solutions for data sovereignty in Indonesia. Section 3 explains requirements analysis based on current legislation and state cyber defence requirements. Section 4 provides data sovereignty requirements. Section 5 presents discussion and potential future work for data sovereignty.

II. Current Approaches

In this section we provide a brief summary of data sovereignty approaches that have been taken by other countries. This can illuminate feasible solutions for Indonesia to better regulate data sovereignty.

A. Approaches to data sovereignty

Many countries have taken concrete steps to safeguard and protect sensitive national data. Polatin-Reuben et al. in [22] highlight BRICS-countries' approaches to data sovereignty such as Brazil, Russia and China. Such countries have been active on data sovereignty requirements against domination of the U.S. global Internet infrastructure. They argue that Chinese and Russian governments have the strongest regulations of data sovereignty regulations for protection their national culture as well as sensitive data, while Brazilian authorities require data sovereignty as a citizenâĂŹs right.

The Brazilian government has passed its "Marco Civil da Internet", which is an Internet "bill of rights". Initially, it would require foreign cloud service providers to store Brazilian data on servers hosted in Brazil and subject to Brazilian law, but the provision later withdrew on its final Internet bill [22]. Similarly, the Russian government has been considering issues on data sovereignty beyond the U.S Internet providers. A new law concerning local servers requires all Internet providers such as Google to store Russian citizens' data on servers inside the country [12]. The government would also propose establishing a national server that would include sensitive and personal data that is subject to Russian laws [16]. In addition, China has strict data localisation laws that require all companies to store Chinese citizens' data on servers located in the country [3]. The same vein, German authorities have been considering data localisation in a number of potential forms such as building out its own Internet infrastructure and keeping its citizens' data within Europe [11].

B. Data Sovereignty Proposals

In partnership with local email providers, the German government encourages its citizens to use a national email services made in Germany, which can help ensure that the German email communications are stored within the country [27]. In Brazil, the government has announced plans to abandon foreign e-mail services for its own domestic email system that utilizes only Brazilian data centres [2].

Due to data leaked by Edward Snowden, the German government also has raised the issue of Internet independence through creating a "Schengen area routing Network" within the European countries. These proposals are still debated within Europe [11].

The German and Brazilian governments have also jointly proposed to build an undersea fiber-optic cable that is intended to channel Internet traffic between South America and Europe, without passing through the U.S. [2] [5]. The two governments have been leading critics of the secret US-NSA program with its "Five-Eyes" intelligence alliance [18]

The Brazilian government would also attempt to build local data clouds and develop domestic contents to keep Brazilian citizens' data within national borders, whilst the German government is attempting to keep its data within European cyberspace [2] [11]. The Russian government also requires foreign Internet providers to locate its servers inside the country and to store user data locally for six months after the data is created [12]. In the same vein, China has also viewed data localisation as an effective measure to control information and keep its citizens' data without reliance on the US Internet providers. It is done through the setting up of the the China's Golden Shield project [28]. It is widely known that some big American Internet services such as Google and Facebook have been blocked in China to regulate its citizen to use local services like Baidu and Weibo [6].

It is clear that some data sovereignty proposals have been identified and implemented in some countries against the domination of the US Internet infrastructures and services. These potential proposals are national email, localised routing of Internet traffic, undersea fiber optic cables and localised data centre.

III. Requirements Analysis

In [18], a set of 25 State Cyber Defence Requirements were identified by Indonesian government, with group discussions and individual sessions to mitigate foreign intelligence services through an adaptive wideband Delphi method. Of these requirements, we selected the following seven that are related to data sovereignty:

1) System and Communications Protection (SCP)
2) National Cryptographic Standards (NCS)
3) Local Applications Platform (LAP)
4) National Infrastructures Platform (NIP)
5) Control of International Traffic (CIT)
6) Domestic Hosting and Domains (DHD)
7) Data Centre Localisation (DCL)

The data sovereignty requirements are examined in detail in Section IV.

A. National Communications Infrastructure

The number of Internet users online is increasing rapidly. According to the Indonesian Internet Service Provider Association (APJII), the number of Internet users will reach from 88.1 million in 2014 to 139 million by 2015 [1]. PT Telkom is Indonesia's largest telecommunications company, with 9.52

million fixed-wire-line customers, 28.69 million fixed-wireless customers, and 137.37 million cellular customers as of June 2014 [26]. PT Indosat is Indonesia's third-largest cellular operator, with more than 59.7 million cellular subscribers [25]. The government of Indonesia retains shares in both companies, including over 50 percent ownership in the case of PT Telkom.

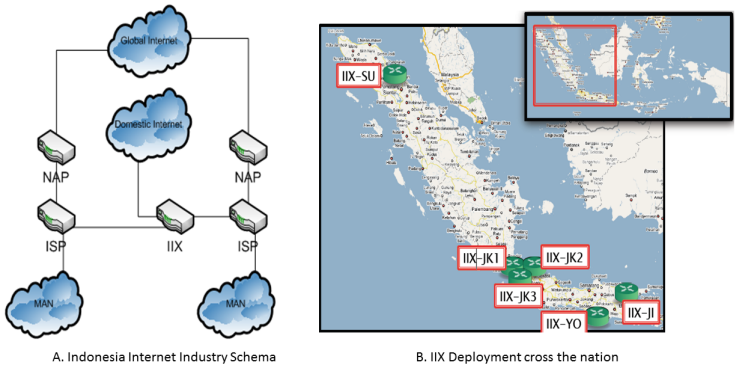
Indonesia has more than 300 Internet Service Providers (ISPs) and Network Access Points [23], which include big operators such as PT Telkom and PT Indosat who own its network infrastructures. The fiber-optic Palapa Ring network is currently being implemented throughout Indonesia to accommodate such a national broadband plan. The Palapa Ring project contains 35,280 kilometres of undersea cable [8]. Many of these submarine cables connect to Singapore, which serves as a major hub for submarine cables used for Internet and telecommunications infrastructures between Asia Pacific and Europe, as shown in Table 1.

In terms of international connections, Indonesia is currently linked to only one intercontinental cable, âĂŞ the South-East Asia-Middle East-Western Europe 3 called the SEA-ME-WE-3, which is the longest optical submarine cable in the world with landing points in Medan and Jakarta. This optical fibre submarine cable runs 39,000 km from Europe, through the Middle East, across to South-east Asia and Korea via China and Japan. Indonesia has no direct connection to the Asia-America Gateway, a 20,000-km cable running from the US West Coast across the Pacific Ocean to South-East Asia [9]. However, recently the new SEA-US submarine cable system is being developed through the five areas and territories of Manado (Indonesia), Davao (Philippines), Piti (Guam), Oahu (Hawaii, United States) and Los Angeles (California, United States). The submarine cable will run approximately 15,000 kilometers in length. This project aims to avoid earthquake prone areas in East Asia, and then to help ensure stable connectivity [17].

It seems clear that the "five-eyes" intelligence alliance such as the British Government Communications Headquarters (GCHQ) through its TEMPORA program can collect all data transmitted to and from the United Kingdom and Northern Europe via the SEA-ME-WE-3. In addition, ASD can cooperate with Singaporean intelligence in accessing and sharing communications carried by submarine cable because all Indonesian international connections connect to Singapore.

TABLE 1 – Indonesia's Submarine Cables in [24]

No.	Indonesia's Submarine Cable List	Owner(s)	Landing Point(s)	
			Domestic	International
1	Jambi-Batam Cable System (JIBA)	Moratelindo	Batam, Jambi,	N/A
2	Jakarta-Bangka-Bintan-Batam-Singapore (B3JS)	Moratelindo	Batam, Bratu Prahu, Jakarta, Pesaren	Singapore
3	SEA-US	RAM Telecom International, Globe Telecom, Hawaiian Telcom, Telkom Indonesia, GTA TeleGuam	Manado	Philippines, United States, Guam
4	Mataram Kupang Cable System (MKCS)	Telkom Indonesia	Ambalawi, Ende, Kupang, Mataram, Saraemee, Sumbawa Besar, Waingapu	N/A
5	JaKa2LaDeMa	Telkom Indonesia	Bali, Banjarmasin, Beculuk, Jimbaran, Ketapang, Mataram, Pankalan,Pontianak, Sangata, Toweli	N/A
6	PGASCOM	PGASCOM	Batam, Kuala Tungkal	Singapore
7	SeaMeWe-5	Telekom Malaysia, Bangladesh Telegraph & Telephone Board, China Mobile, China Telecom, Orange, Myanmar Post and Telecommunication, Saudi Telecom, Sri Lanka Telecom, Telkom Indonesia, TOT, SingTel, Telecom Italia Sparkle, TeleYemen, China Unicom, du, Turk Telekom International, TransWorld Associates (Pvt.) Limited	Batam	Egypt, Yemen, Oman, Italy, Djibouti, United Arab Emirates, Pakistan, Bangladesh, Sri Lanka, Malaysia, India, Myanmar, Thailand, France, Singapore, Saudi Arabia
8	Batam Singapore Cable System (BSCS)	Telkom Indonesia	Batam	Singapore
9	SeaMeWe-3	Orange, BT, KDDI, SingTel, Telecom Italia Sparkle, Telekom Malaysia, OTEGLOBE, AT&T, Belgacom, Communications Authority of Thailand, China Telecom, Deutsche Telekom, Etisalat, Telecom Egypt, CTM, PT Indonesia Satellite Corp., Jabatan Telecom Brunei, KT, Portugal Telecom, Maroc Telecom, PLDT, Saudi Telecom, Sri Lanka Telecom, Turk Telekom, Tata Communications, Chunghwa Telecom, Verizon, KPN, Telekom Austria, SingTel Optus, Telstra, Vietnam Telecom International, Omantel, PCCW, Pakistan Telecommunications Company Ltd., Cyta, eircom, LG Uplus, Softbank Telecom, Telkom South Africa, Rostelecom, Orange Polska, SingTel Optus, Telecom Argentina, Myanmar Post and Telecommunication, Sprint, Vocus Communications, Djibouti Telecom, Embratel, Vodafone	Ancol, Medan	Egypt, Philippines, Greece, India, Vietnam, Hong Kong, Djibouti, Taiwan, United Arab Emirates, United Kingdom, Saudi Arabia, Pakistan, Korea, Turkey, Italy, Malaysia, Sri Lanka, India, Oman, Germany, Japan, Belgium, France, Australia, Myanmar, Thailand, Portugal, China, Singapore, Brunei, Morocco, Cyprus
10	Thailand-Indonesia-Singapore (TIS)	SingTel, Communication Authority of Thailand, Telkom Indonesia	Batam	Singapore, Thailand
11	Dumai-Melaka Cable System	Telkom Indonesia	Dumai	Malaysia
12	Matrix Cable System	Matrix Network Pte., Ltd.	Batam, Jakarta	Singapore
13	Australia-Singapore Cable (ASC)	Nextgen Networks	Jakarta	Australia, Singapore
14	APX-West	SubPartners	Jakarta	Australia, Singapore
15	Moratelindo International Cable System-1 (MIC-1)	Moratelindo	Batam	Singapore
16	Batam-Rengit Cable System (BRCS)	PT. Excelcomindo Pratama	Batam	Malaysia
17	JAKABARE	PT. Indonesia Satellite Corp.	Sungai Kakap, Tanjung Bemban, Tanjung Pakis	Singapore
18	Batam Dumai Melaka (BDM) Cable System	Moratelindo, Telekom Malaysia	Batam, Dumai	Malaysia



A. Indonesia Internet Industry Schema B. IIX Deployment cross the nation

FIGURE 1 – Indonesia Internet Exchange [23]

B. Indonesia Internet eXchange (IIX)

Indonesia has several links to overseas networks and does not have a centralized Internet infrastructure. The APJII manages the Indonesia Internet Exchange (IIX) and the country's first Internet exchange point (IXP), whereas the Indonesia Data Center (IDC) operates the country's second IXP. The government mandates that ISPs must subscribe their IP transit from the network access provider (NAP) as global upstream. The IXPs only serve a local/domestic function between Indonesian ISPs. Moreover, the government will develop 33 IIX nodes in each province, as shown in Figure 1. However, the government should encourage local and global content providers to put or directly peer their servers on IIX [23].

C. International Connectivity

A ISP must has an official registered number that is called the Autonomous System Number (ASN). This number is used for identifying the ISP itself as well as exchanging routing information between neighboring ISPs. The middle layer of nodes in Figure 2 represents major ISPs in Indonesia such as Indosat, Biznet, Telkomnet, Lintasarta, which have upstream

connectivity to international networks. Each ISP has a direct link to international connectivity that indicates a lack of centralised control in relation to the flow of information on the Internet [13].

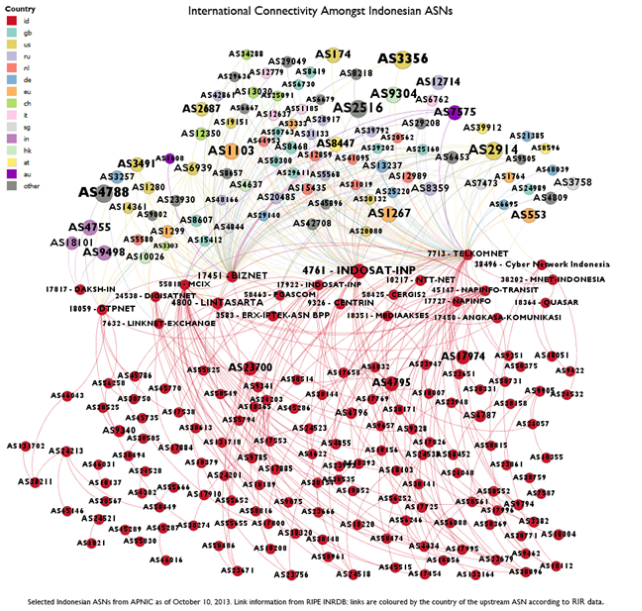


FIGURE 2 – International Connectivity [13]

D. Colocation Data Centre

Currently there are 37 colocation data centers from 16 areas in Indonesia, as shown in Table 2. Most data centers are at Tier 1 or Tier 2 even though some required information is not available. However, a small number of data centers are provided at Tier 3 and Tier 4, which are best equipped to make the significant investment required to guarantee higher security. Since Indonesia has 33 provinces, it is essential to have more colocation data centres provided.

E. Compliance and Regulations

Lack of data protection law leads to the absence of national data protection authority and a loss of control for the government to better protect protect its citizens. However, there are a number of regulations that address data protection requirements as follows:

Law number 11/2008 on Electronic Information and Transaction (EIT Law) Article 26, Telecommunications Law number 36 of 1999 Article 42, Public Information Disclosure Law number 14 of 2008 Article 6 and 17, and Government Regulation number 82/2012 on Electronic System and Transactions Operation have provisions in relation to personal data protection. Moreover, the Government Regulation no 82/2012 Article 17 section 2 states that any Electronic System Operator for the Public Service is obligated to put in place the data center and disaster recovery center in Indonesian territory for the purpose of law enforcement, protection and enforcement of national sovereignty. However, other providers such as non public services are not regulated yet. In addition, it is stated in

TABLE 2 – Colocation Data Centre in Indonesia [14]

No.	Area	Colocation	Provider	Tier Level
1	Ambon	Mitrakom Data Center	Tangara Mitrakom	N/A
2	Bandung	GreenLinks Data Center	Bandung Sinergi Akses Teknologi	N/A
3	Batam	Nusantara Data Center	Mora Telematika Indonesia	3
4	Cimanggis	Biznet Technovillage Data Center	Biznet Networks	3
5	Bogor	Faasri Data Center	Faasri Utama Sakti	4
6	Bogor	Telkomsigma Data Center	Telkom Sigma	3
7	Bekasi	Data Centre Infrastructure	DCI Indonesia	4
8	Serpong	Telkomsigma Data Center	Telkom Sigma	3
9	Denpasar	Nusantara Data Center	Mora Telematika Indonesia	3
10	Jakarta	Biznet MegaPOP	Biznet Networks	2
11	Jakarta	GSD	Dwi Tunggal Putra	N/A
12	Jakarta	NAP Info	Matrix Network & NAP Info Lintas Nusa	N/A
13	Jakarta	Centrin Online	Centrin Online Tbk.	N/A
14	Jakarta	Dhecyber Flow Indonesia	Dhecyber Flow Indonesia	N/A
15	Jakarta	IDCdotCom	NV Utama	N/A
16	Jakarta	NEX Data Center	CBN Nusantara	3
17	Jakarta	The Energy Data Center	Api Metra Graha	N/A
18	Jakarta	JUPITER	JUPITER	N/A
19	Jakarta	NTP	Nexis Inti Persada	N/A
20	Jakarta	VIPNET	VIPNET	N/A
21	Jakarta	CBTP	Cybertechtonic Pratama	N/A
22	Jakarta	Nusantara Data Center	Mora Telematika Indonesia	3
23	Jakarta	Murah-Banget.Com	Interlink Technology	N/A
24	Jakarta	Axarva Data Center	Axarva Media Teknologi	3
25	Jakarta	Cyber Data Center International	Cyber Data Center International	3
26	Jakarta	Goldenfast Network	Jejaring Cepat Indonesia	N/A
27	Kupang	Mitrakom Data Center	Tangara Mitrakom	N/A
28	Makassar	XMedia	Media Inter Data	N/A
29	Manokwari	Mitrakom Data Center	Tangara Mitrakom	N/A
30	Mataram	Mitrakom Data Center	Tangara Mitrakom	N/A
31	Medan	Nusantara Data Center	Mora Telematika Indonesia	3
32	Medan	Kinerja Data Center	Kinerja Indonesia	2
33	Palembang	Nusantara Data Center	Mora Telematika Indonesia	3
34	Surabaya	Omadata Surabaya Data Center	Omadata Surabaya Data Center	N/A
35	Surabaya	XMedia	Media Inter Data	N/A
36	Surabaya	Nusantara Data Center	Mora Telematika Indonesia	3
37	Surabaya	Telkomsigma Data Center	Telkomsigma	3

Article 43 of the regulation, the electronic transaction operator shall keep local transaction data within the country. These regulations would apply to both private and public electronic system providers.

IV. Data Sovereignty Proposals

This paper proposes elements of data sovereignty requirements, which include the assurance of data confidentiality, data integrity, and data availability, as follows:

A. Data Confidentiality

This requirement aims to protect national sensitive data from being disclosed. Public administrations must have the necessary requirements in terms of classified information that needs to be highly protected according to the Public Information Disclosure Act No. 14/2008 and the National Intelligence Act No. 17/2011. To ensure data confidentiality, the most straightforward method is to encrypt all the sensitive data for storage, processing, and transmission. An alternative is to only store unclassified data in cyberspace such as clouds. Some data sovereignty proposals that can be considered are as follows:

1) Secure Encryption Standard: Encryption protects data in transit, at rest, and in other storage. It can be used to safeguard and protect national sensitive data. The widely used end-to-end encryption would make any foreign intelligence services less capable of decrypting national sensitive data.

This proposal relates to the National Cryptographic Standard (NCS) requirement of the 25 Cyber Defence Requirements . This requirement helps ensure that reasonable effort has been made to protect classified information related to the state secrets [18].

B. Data Integrity

This requirement aims to protect data from malicious modification. The use of Encryption is also widely used to better

protect data during storage, processing and transmission. For investigation, it is also necessary to guarantee that all audit data are authentic and considered admissible in court . Data stored in data centers may be subject to modification by insider threats. Thus, the NCS requirement would apply within this security service.

C. Data Availability

This requirement assures that data stored in the Internet are available on each user retrieval request. This requirement is particularly necessary for data at rest in physical servers that provide a Service Level Agreement (SLA). Service providers should provide a guarantee that users' data stored in the data centre can be immediately available whenever required. In particular, it is important to assure the availability of data in case of permanent service outage and force majeure such as war and crime. Some localisation proposals that can be considered are as follows :

1) Localised data storage: Data security depends on factors beyond the physical location of servers. Data localisation capability could be used to identify and prosecute criminal activities. In addition, local data storage helps ensure that reasonable effort has been made to protect users' data from foreign surveillance. Data security depends not only on its geographical location, but also on the actual secure encryption mechanisms used to store the data. However, from security perspective in terms of data availability against force majeure such as war, data centre localization (DDL) would be a feasible way to achieve a data sovereignty requirement.

This proposal is related to Data Centre Localisation (DCL) from the Indonesian Cyber Defence Requirements. This requirement helps ensure that the obligation to place a data centre, and disaster mitigation centre locally must be in place for the purpose of law enforcement, protection and sovereignty of the state and its citizens [18].

2) Localised routing (Indonesia Internet Exchange): Localized routing of Internet traffic would help ensure an Indonesian law enforcement agency can better perform investigation because the data flows are localised within the country, which is subject to national laws. Localised routing helps to control data generated in or passing through the national communications infrastructure.

This proposal is associated with the Control of International Traffic (CIT) requirement. This requirement helps ensure that the government has a means for controlling data, which is intended for destinations outside the country [18].

3) Undersea Cable (Palapa Ring Project): New undersea cables will offer more capabilities to Indonesian law enforcement agencies to access the data flows through the submarine cables. It could minimize risks of foreign surveillance against international backbone dependencies.

This localisation proposal is related to National Infrastructure Platform (NIP) and System and communications Protection (SCP), which can help ensure that national infrastructure such as the backbone optic infrastructures must be utilized in delivering national sensitive data with reasonable security [18].

4) National email (dot ID): National email services should have a higher security standard in comparison to the foreign providers' capabilities. Given the current encryption standard used for national email is not higher than the standard used by most providers, the new mail services will not improve data security. However, the Indonesian law enforcement agencies can access the data because it is stored within national borders, and therefore subject to national legislation that normally contains enforcement exceptions.

This proposal is related to Local Application Platform (LAP) and Domestic Hosting and Domains (DHD), which helps ensure that all local organisations must utilize local applications for data sovereignty in order to keep data traffic within national borders [18].

V. Discussion and Future Work

This study has proposed the initial data sovereignty requirements such as data centre localisation, national routing, national email services and national backbone infrastructure. Data sovereignty requirements may not be solved only using technology proposals. Other aspects such as legal remedies should be considered when technical solutions fail to meet data sovereignty requirements [21].

It is clear that every country should first define data sovereignty requirements. It may be different for every country depending on their capabilities. Since the situation of nation-states and their capabilities may change from time to time, expectations for data security requirements can vary widely between different countries.

Data sovereignty requirements should be made flexible enough to accommodate ICT developments and the government interest in data security. However, data sovereignty requirements raise many questions. Such strong requirements for data sovereignty pose a threat to the global Internet development especially a change in Internet governance structures. Moreover, it would have severe implications for most potential foreign investors and global private sectors.

Continuing diplomatic efforts and international cooperation in relation to data sovereignty in cyberspace are necessary to ensure that there is an agreement between nation-states, and with global private sectors, on how to manage cross border data transfer in cyberspace.

From a technical perspective, the question remains, what are the data sovereignty protocols that need to be established. It is clear that the Indonesian government must build their own best capacity to protect national sensitive data against cyber threats such as foreign intelligence services. However, such intelligence agencies have an important role in protecting their national security. Thus, reasonable efforts should be made by the Indonesian government to attain data sovereignty in cyberspace and this could be the basis for future research.

To ensure the confidentiality of national sensitive data, a reasonable effort is to encrypt all the sensitive data for processing, transmission and storage. In terms of key management,

however, it is challenging to securely distribute the keys to authorised parties when cross border data exists. If necessary, the sensitive data may be kept separately or protected using encryption standards when the data storage is connected to the global system.

Data sovereignty cannot guarantee data security from data breaches, data loss and privacy intrusions. A public administration should employ security best practice for an authentication framework such as two-factor authentication and data leak prevention to help ensure a higher degree of authentication, non-repudiation, and access control.

To provide strong security mechanisms on data availability, there are two most promising approaches, which are provable data possession (PDP) and proof of retrievability (POR) [21]. It would be important to achieve data sovereignty with technical solutions, but it would need a suite of approaches that can help ensure that data sovereignty can be attained.

Ideally, establishing such monitoring and auditing capability using trustworthy mechanisms makes data sovereignty accountable and measurable. While some data sovereignty requirements may be unrealistic to deploy globally across the Internet, it may be practical to satisfy nation-states among standards and regulations concerning data security and management.

ACKNOWLEDGMENT

The authors would like to thank the Ministry of Communications and Information Technology, Indonesia, for supporting this study. Many thanks to Andrew Paverd for the discussions and helpful comments on this manuscript.

REFERENCES

[1] Asosiasi Penyelenggara Jasa Internet Indonesia. Penguna internet indonesia tahun 2014. Available online at: http://www.apjii.or.id/v2/read/content/info-terkini/301/pengguna-internet-indonesia-tahun-2014-sebanyak-88.html, 2014. Accessed 5 April 2015.

[2] Zygmunt Bauman, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and RBJ Walker. After snowden: Rethinking the impact of surveillance. *International Political Sociology*, 8(2):121–144, 2014.

[3] Yusuf Bhana. How data localisation laws may affect global business. Available online at: http://www.preludegroup.co.uk/2014/10/30/how-data-localisation-laws-may-affect-global-businesses/, 2014. Accessed 9 January 2015.

[4] Biswajit Biswal, Sachin Shetty, and Tamara Rogers. Classification based ip geolocation approach to locate data in the cloud datacenters. 2014.

[5] Robin Emmott. Brazil, europe plan undersea cable to skirt u.s. spying. Available online at: http://www.reuters.com/article/2014/02/24/us-eu-brazil-idUSBREA1N0PL20140224, 2014. Accessed 9 January 2015.

[6] Same Frizell. Here are 6 huge websites china is censoring right now. Available online at: http://time.com/2820452/china-censor-web/, 2014. Accessed 9 January 2015.

[7] Dong Lai Fu, Xin Guang Peng, and Yu Li Yang. Trusted validation for geolocation of cloud data. *The Computer Journal*, page bxu144, 2014.

[8] Oxford Business Group. Indonesia: Building capacity for data. Available online at: http://www.oxfordbusinessgroup.com/news/indonesia-building-capacity-data, 2011. Accessed 5 April 2015.

[9] Oxford Business Group. Network news: Improving international connectivity is among the items on the agenda. Available online at: http://www.oxfordbusinessgroup.com/analysis/network-news-improving-international-connectivity-among-items-agenda, 2014. Accessed 5 April 2015.

[10] Bamba Gueye, Artur Ziviani, Mark Crovella, and Serge Fdida. Constraint-based geolocation of internet hosts. *Networking, IEEE/ACM Transactions on*, 14(6):1219–1232, 2006.

[11] Jonah Force Hill. The growth of data localization post-snowden: Analysis and recommendations for us policymakers and business leaders. In *The Hague Institute for Global Justice, Conference on the Future of Cyber Governance*, 2014.

[12] Ilya Khrennikov. Google to visa face russia rules, boon to local data centers. Available online at: http://www.bloomberg.com/news/2014-09-25/google-to-visa-face-russia-data-rules-in-boon-to-local-operators.html, 2014. Accessed 9 January 2015.

[13] The Citizen Lab. IGF 2013: An overview of indonesian internet infrastructure and governance. Available online at: https://citizenlab.org/2013/10/igf-2013-an-overview-of-indonesian-internet-infrastructure-and-governance/, 2013. Accessed 9 January 2015.

[14] Data Centre Map. Colocation indonesia. Available online at: http://www.datacentermap.com/indonesia/, 2015. Accessed 9 January 2015.

[15] Tim Maurer, Robert Morgus, Isabel Skierka, and Mirko Hohmann. Technological sovereignty: Missing the point? Available online at: http://www.newamerica.org/downloads/Technological_Sovereignty_Report.pdf, 2014. Accessed 9 January 2015.

[16] Evgency Morozov. WhoâĂŹs the true enemy of internet freedom - China, Russia, or the US? Available online at:http://www.theguardian.com/commentisfree/2015/jan/04/internet-freedom-china-russia-us-google-microsoft-digital-sovereignty, 2015. Accessed 9 January 2015.

[17] NEC. Sea-us: Global consortium to build cable system connecting indonesia, the philippines, and the united states. Available online at: http://uk.nec.com/en_GB/press/201408/20140828_01.html, 2014. Accessed 5 April 2015.

[18] Y. Nugraha, I. Brown, and A.S. Sastrosubroto. An adaptive wideband delphi method to study state cyber-defence requirements. *Emerging Topics in Computing, IEEE Transactions on*, PP(99):1–1, 2015.

[19] Yudhistira Nugraha and Ashwin Sasongko Sastrosubroto. National cybersecurity policy assessment toward a smart nation. pages 101–109. e-Indonesia Initiatives Forum, 2014.

[20] The Australian Department of Defence. The slides that show australian attempts to monitor yudhoyono's phone. Available online at: http://www.theguardian.com/world/interactive/2013/nov/18/slides-australian-yudhoyono-phone-indonesia, 2009. Accessed 9 January 2015.

[21] Zachary NJ Peterson, Mark Gondree, and Robert Beverly. A position paper on data sovereignty: the importance of geolocating data in the cloud. In *Proceedings of the 3rd USENIX conference on Hot topics in cloud computing*, pages 9–9. USENIX Association, 2011.

[22] Dana Polatin-Reuben and Joss Wright. An internet with brics characteristics: Data sovereignty and the balkanisation of the internet. In *4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14)*. USENIX Association, 2014.

[23] Harijanto Pribadi. Indonesia internet exchange. PowerPoint Presentation by Harijanto Pribadi, Department Head of IIX APJII, Available online at: https://citizenlab.org/wp-content/uploads/2013/10/IIX-APJII2012-APNIC34-Final.pptx, 2012. Accessed 9 January 2015.

[24] PriMetrica. Submarine cable map : Indonesia. Available online at: http://www.submarinecablemap.com/#/country/indonesia, 2013. Accessed 9 January 2015.

[25] PriMetrica. IndonesiaâĂŹs third largest mobile phone operator by subscribers. Available online at: https://www.telegeography.com/products/commsupdate/articles/2014/05/09/indosat-surges-back-into-profit-after-years-of-losses/, 2014. Accessed 5 April 2015.

[26] PT Telkom Indonesia. Kinerja telkom semester i/2014. Available online at: http://www.telkom.co.id/kinerja-telkom-semester-i2014-tumbuh-meyakinkan.html, 2014. Accessed 5 April 2015.

[27] Amar Toor. Brazil and germany make moves to protect online privacy, but experts see a troubling trend toward balkanization. Available online at: http://www.theverge.com/2013/11/8/5080554/nsa-backlash-brazil-germany-raises-fears-of-internet-balkanization/, 2013. Accessed 9 January 2015.

[28] Joss Wright. Regional variation in chinese internet filtering. *Information, Communication & Society*, 17(1):121–141, 2014.