STRATEGI BADAN SIBER DAN SANDI NASIONAL DALAM MENGHADAPI ANCAMAN SIBER TERHADAP SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

NATIONAL CYBER AND CRYPTO AGENCY STRATEGY IN FACING CYBER THREATS TO ELECTRONIC BASED GOVERNMENT SYSTEMS

Muh. Fachrul Febriansyah[2], Agus Adriyanto[3], Fetri Miftach[4]

PRODI PEPERANGAN ASIMETRIS FAKULTAS STRATEGI PERTAHANAN UNIVERSITAS PERTAHANAN
(fachrulmuhammad@gmail.com)

Abstrak – Perkembangan teknologi informasi dan komunikasi (TIK) telah membawa manusia kepada era baru dalam berkomunikasi. Munculnya internet pada tahun 1990-an telah merevolusi dunia hingga saat ini. Seiring dengan perkembangan TIK dan internet, setiap negara kemudian mulai memanfaatkan teknologi tersebut untuk meningkatkan pelayanan publik di negaranya masing-masing, tidak terkecuali Indonesia. Indonesia mulai mengembangkan proyek e-government pada tahun 2003 yang atas dasar Inpres No. 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan *E-Government*. Dalam perkembangannya, ditemukan hambatan dan masalah serta perlunya pengamanan terhadap sistem e-gov tersebut. Hingga pada akhir 2018 dimana pemerintah menerbitkan Perpres No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE). Perpres semakin mengakselarasi penerapan *e-gov* / SPBE di Indonesia menuju *i-government (integrated government)*. Namun tentunya, seiring dengan penerapan SPBE secara nasional maka ancaman siber pun akan semakin besar. BSSN merupakan salah satu anggota dari Tim Koordinasi SPBE Nasional yang memiliki tanggung jawab dalam pengamanan SPBE dan harus menyusun regulasi, kebijakan dan strategi dalam mengamankan SPBE Nasional. Penelitian ini membahas strategi BSSN dalam mengamankan SPBE dari ancaman siber serta hambatan dan tantangannya. Penelitian ini menggunakan metode kualitatif dengan pendekatan fenomenologi. Data dari informan diperoleh melalui wawancara dan studi literatur. Penelitian ini menggunakan teori ilmu pertahanan, teori strategi, konsep e-government dan konsep ancaman siber. Hasil penelitian ini ditemukan bahwa penerapan strategi pengamanan SPBE oleh BSSN mengalami beberapa hambatan, yaitu regulasi atau kebijakan yang sedang dirancang sehingga strategi belum bisa diimplementasikan. Oleh karena itu, kesimpulan dari penelitian ini adalah penerapan SPBE di Indonesia sudah mulai berjalan namun pengamanannya sendiri masih belum siap dikarenakan keterbatasan regulasi dan strategi yang masih belum berjalan.

Kata Kunci: ancaman siber, Badan Siber Dan Sandi Nasional, keamanan, Sistem Pemerintahan Berbasis Elektronik, strategi

Abstract *– The development of information and communication technology (ICT) has brought humans to a new era in the way to communicate. The advent of the internet in the 1990s has revolutionized the world today. Along with the development of ICT and the internet, each country then began to exploit the technology to improve public services in their respective countries, including Indonesia. Indonesia began to develop e-government projects in 2003 based on Presidential Instruction Number*

[2] Program Studi Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan
[3] Program Studi Damai dan Resolusi Konflik, Fakultas Keamanan Nasional, Universitas Pertahanan
[4] Program Studi Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan

3 of 2003 concerning National Policies and Strategies for E-Government Development. In its development, obstacles and problems and the need for security of the e-gov system were discovered. End of 2018 the Government issued Presidential Regulation Number 95 of 2018 regarding Electronic-Based Government Systems (SPBE). The Presidential Regulation further accelerates the implementation of e-gov / SPBE in Indonesia towards i-government (integrated government). However, along with the national application of SPBE, the cyber threat is getting worse greater. BSSN is a member of the National SPBE Coordinating Team which has the responsibility of securing SPBE and preparing regulations, policies, and strategies in securing the National SPBE. This research analyzes BSSN's strategy in securing SPBE as a defense against cyber threats. The research method used is qualitative with a phenomenological approach. Data from informants was obtained through interviews and literature studies. This research uses the theory of defense science, strategy theory, e-government concepts, and the concept of cyber threats. The results of this study found that the implementation of the SPBE security strategy by BSSN experienced several obstacles, namely regulations or policies that were being designed so that the strategies could not be implemented. This study concludes that the application of SPBE in Indonesia has begun to run, but the security itself is still not ready due to limited regulations and strategies that are still not running.

Keywords: *cyber threats, National Cyber And Crypto Agency, e-government, security, strategy*

Pendahuluan

Perkembangan teknologi informasi dan komunikasi (TIK) telah memunculkan era dimana manusia dapat berkomunikasi tanpa batas atau dalam bahasa lain yaitu *borderless*. Era yang dimaksud adalah penggunaan internet yang dapat memberikan manusia sebuah kemudahan dalam mengakses data dan informasi dimana saja dan kapan saja. Kecanggihan teknologi informasi dan komunikasi tersebut kemudian juga diadaptasi di dalam segala aspek kehidupan umat manusia, tidak terkecuali kehidupan berbangsa dan bernegara.

James Cash dalam Richardus Eko Indrajit (2013) membagi perkembangan teknologi informasi dan komunikasi ke dalam empat fase atau era. [5]

Fase pertama dimulai pada tahun 1960-an dimana era komputerisasi mulai digunakan dimana-mana. Pada era ini, perusahaan seperti *International Business Machines Corporation* (IBM) mulai menggunakan komputer di dalam industri untuk meningkatkan efisiensi, baik dari segi waktu maupun biaya. Hal ini menjadi salah satu bukti konkrit bahwa teknologi informasi dan komunikasi dapat memudahkan kehidupan manusia dengan meningkatkan efisiensi. Pada era itu juga, kebanyakan perusahaan-perusahaan yang bergerak di bidang teknologi mulai membeli perangkat

[5] Richardus Eko Indrajit, "Evolusi Perkembangan Teknologi Informasi", dalam https://www.academia.edu/14351956/Evolusi_Perkembangan_Teknologi_Informasi, 2013, diakses pada 12 Juni 2019.

komputer dengan jumlah besar untuk membantu kegiatan administrasi di dalam perusahaan.[6]

Era kedua adalah era teknologi informasi dimana era mulai terjadi revolusi di bidang teknologi dan informasi. Era ini terjadi pada tahun 1970-an dimana PC (perangkat komputer yang kita kenal saat ini) mulai menggantikan *mini computer* sebagai alternatif. Di sebuah perusahan, *Personal Computer* atau PC digunakan oleh seorang manajer dalam mendapatkan data atau informasi di dalam perusahaan yang telah diolah dengan menggunakan kecepatan yang sama dengan *mini computer*. Jika *mini computer* di era sebelumnya digunakan perusahaan khusus untuk mengolah data dan informasi, maka di era ini PC digunakan setiap individu di dalam perusahaan untuk mengolah *database*, *spreadsheet* hingga *data processing*. Efisiensi dan efektivitas kerja kemudian akan semakin tercapai dibandingkan dengan perusahaan yang hanya mengelola pekerjaannya dengan cara manual.

Selanjutnya, era ketiga yaitu era sistem informasi dimana manajemen organisasi modern mulai terjadi pada tahun 1980-an. Jika sebelumnya menekankan pada unsur teknologi, maka era manajemen organisasi modern lebih kepada sistem informasi, dimana komputer merupakan bagian dari sistem informasi tersebut. Komputer dan teknologi informasi yang digabungkan dengan proses, prosedur, struktur organisasi dan sumber daya manusia yang ada di organisasi atau perusahaan dapat membentuk sistem informasi yang baik sehingga menjadi organisasi atau perusahaan yang berhasil secara strategis.[7]

Terakhir adalah era globalisasi informasi yang merupakan evolusi bagi umat manusia. Evolusi ini ditandai dengan kemunculan internet di awal tahun 1990-an. Bahkan pada tahun 1996 di San Fransisco, para praktisi dan ahli teknologi menyatakan bahwa mereka tidak pernah menduga perkembangan internet hingga menjadi semaju sekarang. Teknologi informasi dan komunikasi sangat sulit untuk dihentikan karena sifatnya yang *borderless* atau melewati batas-batas negara seperti yang telah disebutkan sebelumnya.

Selain perusahaan-perusahaan yang bergerak di bidang teknologi, internet

[6] *Ibid.,* hlm. 2.

[7] *Ibid.,* hlm. 5-6.

kemudian mulai digunakan oleh pemerintah suatu negara untuk meningkatkan layanan publiknya. Setiap negara mulai merancang suatu sistem yang berguna bagi kehidupan masyarakat sebagai bagian dari pelayanan publik yang diberikan oleh pemerintah. Sistem ini dikenal dengan istilah *e-government* (*electronic government*) atau sistem pemerintahan berbasis elektronik.

E-government merupakan komitmen dan inisiatif pemerintah untuk meningkatkan hubungannya dengan masyarakat dan sektor bisnis melalui layanan yang efisien dan efektif menggunakan (TIK). E-government tidak hanya memberikan manfaat seperti layanan yang lebih cepat, lebih murah, dapat dipercaya dan dapat diandalkan oleh masyarakat dan sektor bisnis, tetapi juga menawarkan potensi untuk membentuk kembali sektor publik dan membangun kembali hubungan antara masyarakat, bisnis dan pemerintah dengan memungkinkan adanya komunikasi terbuka (transparan), partisipasi dan dialog publik dalam merumuskan peraturan nasional.[8]

Di Indonesia sendiri, *e-government* diterapkan berdasarkan Instruksi Presiden Republik Indonesia Nomor 6 Tahun 2001 tentang Pengembangan dan Pendayagunaan Telematika di Indonesia dan Instruksi Presiden Republik Indonesia Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan *E-Government*. Payung hukumnya juga telah dirilis melalui Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. *E-Government* atau dalam bahasa Indonesia yaitu sistem pemerintahan berbasis elektronik yang mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan dan akuntabel serta pelayanan publk yang berkualitas dan terpercaya.[9]

Munculnya revolusi industri 4.0 menuntut Indonesia untuk mengadaptasi teknologi-teknologi masa depan yang semakin meningkatkan efisiensi antara pemerintah dengan warga negaranya. Berikut beberapa yang teknologi yang akan coba diadaptasi ke depannya oleh pemerintah Indonesia pada sistem pemerintahan berbasis elektronik:[10]

[8] W. Tan & R. Subramaniam, "E-Government: Implementation Policies and Best Practices from Singapore", *Electronic Government Strategies and Implementation*, 2005, hlm. 305-324.

[9] Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.

[10] *Ibid*.

a. *Mobile Internet*
b. *Cloud Computing*
c. *Internet of Things (IoT)*
d. *Big Data Analysis*
e. *Artificial Intelligence (AI)*

Seiring dengan perkembangan layanan *e-governmen*t yang mulai memanfaatkan teknologi-teknologi masa depan diatas, sistem *e-government* menjadi target potensial bagi para penyerang siber yang biasa disebut sebagai *hacker*. Intrusi terhadap sistem jaringan *e-governmen*t dapat menganggu layanan *e-governmen*t kapan saja jika tidak diamankan dengan baik. Sebuah studi keamanan *e-government* pada tahun 2005 melaporkan bahwa 82% dari situs *e-governmen*t di seluruh dunia rentan terhadap serangan siber. Pada tahun 2007 juga dilaporkan bahwa negara-negara besar seperti Amerika Serikat menjadi target serangan siber paling banyak dengan bentuk serangan *denial of service* (DoS).[11]

Indonesia sendiri tentunya memiliki kerentanan yang sama jika menggunakan perspektif bahwa tidak ada sistem yang aman. Sesuai dengan Perpres RI Nomor 95 Tahun 2018 Pasal 41 ayat (2), dalam penerapan keamanan dan menyelesaikan permasalahan keamanan sistem pemerintahan berbasis elektronik, penyelenggaran tugas tersebut dipegang oleh lembaga pemerintah yang bergerak di bidang keamanan siber, dalam hal ini adalah Badan Siber dan Sandi Negara (BSSN).[12]

BSSN wajib melakukan pengamanan karena ancaman dan serangan siber dapat menganggu layanan *e-government* dimana terdapat banyak lalu lintas data dan informasi terjadi di dalamnya. Sehingga dapat dikatakan bahwa *e-government* merupakan bagian dari infrastruktur informasi kritis nasional yang harus dilindungi. Serangan siber terhadap layanan *e-government* dianggap dapat mengancam keamanan nasional karena banyaknya pihak-pihak yang terlibat di dalamnya.

Berdasarkan hal tersebut, banyaknya pihak yang berkepentingan dan terlibat dalam layanan sistem *e-government*, baik penyedia layanan yaitu pemerintah maupun *user* atau pengguna dari masyarakat dan pebisnis akan mengalami kerugian yang besar jika terjadi serangan siber, sehingga stabilitas

[11] Jensen J. Zhao & Sherry Y. Zhao, "Opportunities and Threats: A Security Assessment of State E-Government Websites", *Government Information Quarterly*, Vol. 8, No. 5, 2010, hlm. 49-56.

[12] Perpres No. 95, Op. Cit, ayat (2).

keamanan nasional negara menjadi terganggu. Permasalahan terbesar dalam hal ini adalah Indonesia akan mulai mengadaptasi teknologi masa depan namun kompleksitas ancaman siber juga semakin meningkat. Indonesia tentunya harus meningkatkan pertahanannya melalui pengamanan yang dilakukan oleh BSSN pada sistem pemerintahan berbasis elektronik.

Berdasarkan permasalahan diatas, maka peneliti akan membahas mengenai perkembangan serta hambatan-hambatan pada penerapan SPBE di Indonesia saat ini dan strategi pengamanan yang dilakukan oleh BSSN terhadap SPBE Nasional dengan harapan dapat memberikan manfaat bagi *stakeholder* terkait berupa strategi pengamanan SPBE yang tentunya dapat dijadikan referensi dalam pengamanan SPBE Nasional.

Metode Penelitian

Penelitian ini menggunakan metode penelitian kualitatif melalui desain penelitian fenomenologi. Menurut Creswell (2010), fenomenologi merupakan pendekatan yang berasal dari filosofi dan psikologi yang mana mendeskripsikan pengalaman hidup suatu individu tentang sebuah fenomena, sebagaimana yang diceritakan oleh pelaku. Pendekatan fenomenologi juga digunakan untuk menganalisis suatu fenomena yang telah terjadi sehingga dapat menemukan penyelesaian terbaik dari masalah-masalah yang belum terselesaikan.[13]

Fenomenologi dipilih karena ancaman siber telah ada sejak lama dan bentuknya semakin berkembang setiap waktunya sehingga sistem pemerintahan berbasis elektronik membutuhkan pengamanan melalui strategi yang dibuat oleh Indonesia. Oleh karena itu, Badan Siber dan Sandi Negara (BSSN) dalam hal ini sebagai leading sector dan agensi siber di Indonesia harus membuat strategi untuk menanggulangi ancaman siber tersebut yang juga merupakan bagian dari bentuk ancaman non-militer.

Teknik pengumpulan data yang dilakukan dalam penelitian ini adalah wawancara dalam bentuk semi terstruktur atau juga disebut dengan *in-depth interview*, studi literatur dan dokumentasi. Data yang telah

[13] John W. Creswell, Research Design: Pendekatan Kualitatif, Kuantitatif dan Mixed, (Yogyakarta: PT. Pustaka Pelajar, 2010).

dikumpulkan selanjutnya diuji keabsahannya pada tahap kredibilitas yaitu melalui teknik triangulasi.

Setelah data dikumpulkan dan diuji keabsahannya, peneliti kemudian menganalisa data tersebut menggunakan teknik analisa data *interactive model* dari Miles and Huberman yang mana terdiri dari 3 (tiga) tahapan, yaitu *data condensation* (kondensasi data), *data display* (penyajian data), dan *drawing/verifying conclusions* (penarikan kesimpulan).[14]

Hasil dan Pembahasan

Perkembangan Sistem Pemerintahan Berbasis Elektronik di Indonesia

Menurut Richardus Eko Indrajit yang mengutip dari Pemerintah Italia, terdapat beberapa kata kunci penting yang berkaitan dengan istilah *e-government*. Pertama, teknologi informasi dan komunikasi (TIK) yang merupakan sarana yang digunakan dalam membangun sebuah sistem *e-government*. Kedua, pemerintah selaku aktor yang menjalankan, menyelenggarakan dan mengadaptasi kegiatan *e-government*. Ketiga, administrasi, yang merupakan kegiatan yang dalam hal ini merupakan pemberian pelayanan publik melalui *e-government*.[15] Ketiga poin nantinya akan digunakan untuk menganalisis perkembangan SPBE di Indonesia.

Adapun pendapat Kepala Sub-Direktorat Tata Kelola Sistem Elektronik Pemerintahan Kominfo, Pancat Setyantana yang menyatakan bahwa sistem pemerintahan berbasis elektronik di Indonesia pertama kali diawali pada tahun 2003 dimana ketika itu pada masa pemerintahan Ibu Megawati dikeluarkan sebuah Inpres atau Instruksi Presiden No. 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan *E-Government*. Inpres tersebut merupakan hasil manifestasi yang menjadi bukti dari pemerintah dalam menyelenggarakan tata kelola pemerintahan yang memanfaatkan infrastruktur teknologi informasi dan komunikasi (TIK).

Pancat melanjutkan bahwa pada tahun 2003, regulasi yang ada tidak banyak dibuat. Namun, dengan adanya Inpres tersebut setidaknya *e-government*

[14] Matthew B. Miles, A. Michael Huberman & Johnny Saldana, Qualitative Data Analysis: A Methods Sourcebook, (Arizona: SAGE Publications, Inc.), hlm. 31-32.

[15] Richardus Eko Indrajit, "Electronic Government", dalam https://www.academia.edu/30100450/Electronic_Government, 2016, diakses pada 9 Juni 2019.

di Indonesia sendiri sudah mulai jalan. Setelah Inpres tersebut diterbitkan, para pejabat pemerintah daerah kemudian mulai mengambil langkah-langkah untuk melaksanakan penerapan *e-government* di daerahnya masing-masing. Para pejabat daerah kemudian berkoordinasi dengan Kementerian Komunikasi dan Informatika ketika itu untuk merumuskan strategi penerapan *e-government* dalam skala nasional.

Perkembangan *e-government* terus meningkat dengan mengacu pada penyelenggaraan pemerintahan yang terbuka, transparan, dan efektif. Pada tahun 2008 Pemerintah kemudian mengeluarkan Undang-Undang No. 14 tahun 2008 tentang Keterbukaan Informasi Publik. Publik berhak menerima data dan informasi yang disajikan oleh pemerintah baik secara elektronik maupun non-elektronik dengan fakta dan keterangan yang bersifat nyata dan transparan. Informasi yang sifatnya publik dan diterbitkan oleh pemerintah harus sesuai dengan Undang-Undang tersebut karena menyangkut kepentingan publik.

Kemudian, beberapa peraturan atau Undang-Undang dikeluarkan oleh pemerintah dengan tujuan mendukung penerapan *e-government* secara nasional. Dilanjutkan pada tahun 2009 dimana Undang-Undang No. 25 tahun 2009 tentang Pelayanan Publik dan Undang-Undang No. 43 tahun 2009 tentang Kearsipan diterbitkan. Lalu, Undang-Undang No. 23 tahun 2014 tentang Pemerintahan Daerah. Peraturan-peraturan tersebut telah menunjan perkembangan pengimplementasian *e-government* pada tingkat nasional. Namun kenyataannya, pembangunan pembangunan *e-government* atau sistem pemerintahan berbasis elektronik pada saat itu masih bersifat sektoral sehingga terjadi kehambatan.

Jika mengacu pada poin-poin penting *e-government* yang telah dijelaskan sebelumnya, pelaksanaan *e-government* atau SPBE di Indonesia telah berjalan sebagaimana mestinya. Poin pertama yaitu teknologi informasi dan komunikasi. Sejak Inpres No. 3 tahun 2003 dikeluarkan oleh Presiden, pelaksanaan *e-government* telah menggunakan TIK sebagai penghubung antara pemerintah, masyarakat dan pihak bisnis.

Kemudian poin kedua yaitu pemerintah selaku aktor penyelenggara *e-government*. Pada tahun 2003, penyelenggaraan e-government lebih banyak dipegang oleh Kominfo sebagai

instansi penyedia layanan berbasis aplikasi dan situs. Namun, dengan adanya

Perpres No. 95 tahun 2018, penyelenggaraan *e-government* atau SPBE akan dilakukan oleh Tim Koordinasi SPBE Nasional yang merancang tata kelola penerapan SPBE Nasional untuk diterapkan di kementerian/lembaga dan daerah.

Poin terakhir adalah administrasi. Dengan adanya *e-government* tentunya kegiatan administrasi diharapkan dapat berjalan dengan bersih, efektif dan efisien. Maka dari itu, sejak tahun 2012, Kominfo telah membuat program bernama Pemeringkatan *E-Government* Indonesia (PeGI) untuk mengukur dan mengevaluasi penerapan SPBE di tiap kementerian/lembaga dan daerah. Program ini merupakan wujud dari pembinaan dan pengawasaan terkait implementasi *e-government* atau SPBE di setiap kementerian/lembaga dan daerah.

Hambatan Tata Kelola Sistem Pemerintahan Berbasis Elektronik

Menurut hasil wawancara dengan informan yang merupakan Kepala Seksi Tata Kelola Sistem Elektronik Kominfo, Jusuf A. Simatupang, beberapa hambatan yang dialami pemerintah dalam penerapan e-government di Indonesia adalah sebagai berikut:

Luas Wilayah Indonesia

Luas wilayah Indonesia yang sangat luas menimbulkan gap yang terlalu tinggi

Infrastruktur

Dengan kondisi wilayah Indonesia yang sangat luas tadi tentunya menimbulkan ketimpangan, salah satunya infrastruktur. Menurut informan, beberapa waktu lalu dilakukan program Pemeringkatan *E-Government* dimana Kominfo melakukan asesmen atau penilaian terhadap *e-government* di wilayah Indonesia Barat dan Timur. Hasilnya, beberapa infrastruktur di wilayah Timur masih sangat tertinggal dibandingkan dengan wilayah Barat.

Sumber Daya Manusia (SDM)

Walaupun *e-government*, telah diinisiasi sejak tahun 2003, namun permasalahan mengenai kompetensi SDM masih sering ada. Saat ini, pemerintah masih jarang memiliki SDM yang cakap dalam bidang tersebut. Pemahaman mengenai e-government pun masih belum merata di tiap daerah sehingga masih menghambat perkembangan *e-government* hingga saat ini.

Pemerataan

Hingga tahun 2018, pemerataan penerapan *e-government* di berbagai instansi pemerintah pusat dan pemerintah daerah masih menjadi masalah dan hambatan. Menurut informan dari Kominfo, masih banyak kementerian/lembaga maupun pemerintah daerah yang belum mau menerapkan *e-government*. Kondisi ini yang membuat pembangungan SPBE yang sedikit bersifat sektoral.

Integrasi dan Interoperabilitas

Dengan pengembangan SPBE yang dilakukan masing-masing kementerian/lembaga, tentunya integrasi dan interoperabilitas menjadi sulit untuk dilakukan. Pembuatan arsitektur pun akan sangat memakan waktu demi pengintegrasian data.

Pemborosan Anggaran

Selama kurun waktu dari tahun 2003 hingga 2018, masing-masing kementerian/lembaga dan pemerintah daerah yang mengembangkan SPBE nya telah membuat puluhan bahkan ratusan aplikasi untuk penyelenggaraan pemerintahan, namun aplikasi-aplikasi tersebut hanya sedikit yang digunakan sehingga terjadi pemborosan anggaran.

Berbagai hambatan dan masalah penerapan SPBE diatas menjadi tantangan bagi pemerintah dalam meningkatkan pelayanan publik dan administasi melalui SPBE. Untuk masalah wilayah Indonesia yang sangat luas dan infrastruktur yang belum merata, solusinya adalah Palapa Ring. Palapa Ring sendiri merupakan sebuah mega proyek ini akan mengintegrasikan jaringan telekomunikasi yang ada di seluruh wilayah Indonesia melalui pembangunan serat optik nasional.

Setidaknya, pemerataan pada infrastruktur jaringan tidak lagi mengalami ketimpangan antara wilayah barat dan timur. Informan dari Kominfo berpendapat bahwa ketika diadakan program Pemeringkatan *E-government* tahun 2016, perbedaan kecepatan jaringan internet terlihat jelas dimana wilayah barat telah memiliki kecepatan hingga puluhan mbps sementara di wilayah timur masih pada satuan kbps.

Kemudian, pada aspek manajemen sumber daya manusia perlu dilakukan beberapa proses demi terbentuknya SDM yang bermutu bagi tata kelola SPBE. Perencanaan, pengembangan, pembinaan dan pendayagunaan SDM dilakukan oleh masing-masing pimpinan kementerian/lembaga dan pemerintah pusat dan melakukan koordinasi dengan Kemenpan RB.

Hambatan berikutnya yaitu integrasi data dan interoperabilitas data yang dapat diatasi melalui proyek Satu Data dan Jaringan Intra Pemerintah. Seluruh data yang ada di pemerintah pusat dan pemerintah daerah nantinya akan ditempatkan dalam satu 'wadah' sehingga membentuk *big data* SPBE nasional. Untuk interoperabilitas data, jaringan intra pemerintah akan berguna untuk menjaga keamanan jaringan pada saat pengiriman data antara pemerintah pusat dan pemerintah daerah.

Masalah anggaran menjadi masalah terakhir dari tata kelola penerapan SPBE di Indonesia. Hal ini bisa diatasi dengan percepatan pembuatan aplikasi umum dan aplikasi khusus SPBE. Tidak ada lagi instansi-instansi pemerintah yang membangun aplikasinya sendiri-sendiri sehingga terjadi inefisiensi dalam penggunaan anggaran. Dalam hal pembuatan aplikasi umum dan aplikasi khusus merupakan tanggung jawab Kominfo, maka dari itu Kominfo wajib mencegah ataupun menghentikan pembangunan dan pengembangan aplikasi sejenis yang sedang dikerjakan.

Kerentanan Keamanan Sistem Pemerintahan Berbasis Elektronik

Kerentanan keamanan SPBE dari ancaman siber juga tidak bisa terlepas begitu saja. Adanya sistem baru dengan standar keamanan yang baik menjadi area bermain tersendiri bagi para *hacker* dalam melakukan serangan siber terhadap SPBE. Area risiko SPBE juga perlu dianalisis lebih dalam agar mengetahui daerah mana saja yang perlu diamankan. Menurut informan dari BSSN, hilangnya data elektronik pada pusat data atau terjadinya kasus dimana aplikasi dan situs tidak dapat diakses pada saat-saat penting, sebagai contoh jika terjadi serangan DDoS, *spoofing* ataupun *deface* maka hal tersebut dapat berdampak pada keberlangsungan layanan pemerintah, khususnya yang berbasis SPBE.

Kegagalan sistem dapat berdampak pada kerugian finansial dikarenakan besarnya biaya yang telah dikeluarkan oleh pemerintah. Contoh jika serangan mengenai sistem perizinan, ekspor/impor, pajak, *e-procurement* dan lain-lain. Imbas dari terganggunya sistem dan terjadi manipulasi informasi pada SPBE dapat menimbulkan dampak ketidakpercayaan masyarakat pada integritas layanan dan kebijakan pemerintah.

Perlu diketahui bahwa saat ini keamanan sistem informasi pemerintah

masih sangat rentan terhadap ancaman siber. Berdasarkan hasil audit yang dilakukan oleh Pusat Pengkajian dan Pengembangan Teknologi BSSN tahun 2016 terhadap 66 (enam puluh enam) sistem informasi dan 16 (enam belas) instansi pemerintah, ditemukan hasil dan presentase sebagai berikut: 56% resiko tinggi, 30% resiko sedang dan 14% resiko rendah. Ini tentunya menjadi masalah bagi pemerintah Indonesia dimana aplikasi dan situsnya memiliki tingkat kerentanan yang cukup tinggi dalam hal keamanan informasi.[16]

Lalu pada tahun 2017 dimana persentase tingkat kerentanan sudah mulai berkurang pada resiko tinggi. Audit dilakukan pada 87 (delapan puluh tujuh) sistem informasi (bertambah 11 dari tahun sebelumnya) dan 21 (dua puluh satu) instansi pemerintah (bertambah 5 dari tahun sebelumnya. Hasilnya, 35% resiko tinggi, 34% resiko sedang dan 26% resiko rendah.[17] Walaupun kerentanan tersebut tidak hilang sepenuhnya, namun tentunya dapat dilihat bahwa resiko kerentanan tersebut dapat menurun dan akan terus seperti itu. Pendapat bahwa tidak ada yang 100% aman memang betul adanya. Mengingat bahwa SPBE merupakan proyek pemerintah yang membutuhkan koordinasi tiap instansi, maka keamanan SPBE pun tentunya membutuhkan kolaborasi dari setiap elemen keamanan siber dimana BSSN sebagai *leading sector*.

Strategi Pengamanan BSSN terhadap Sistem Pemerintahan Berbasis Elektronik

Ada beberapa aspek yang menjadi fokus BSSN dalam mengamankan SPBE yaitu mengenai keamanan data/informasi, keamanan aplikasi, keamanan jaringan, dan keamanan infrastruktur. Keempat aspek tersebut mengarah pada pembentukan standar dan kriteria keamanan SPBE.

Sebelum menyusun sebuah strategi, ada beberapa hal yang perlu diperhatikan dalam manajemen strategis. Menurut F. R. David manajemen strategis terdiri dari tiga tahapan, yaitu perumusan strategi, implementasi strategi dan evaluasi strategi.[18] Tahap pertama yaitu

[16] Anggrahito, "Penerapan Vulnerability Assessment dan Penetration Test Bagi Pelaksanaan Audit Keamanan Informasi Sektor Pemerintah", dalam https://govcsirt.bssn.go.id/download/Penerapan-VA-dan-Pentest-bagi-Audit-Kaminfo-Sek.Pem-signed.pdf, 10 Agustus 2018, diakses pada 10 Januari 2020.

[17] *Ibid*.

[18] Fred R. David, Strategic Management: Concepts and Cases, (New Jersey: Prentice Hall, 2011), hlm. 6-7.

perumusan strategi dimana dalam konteks perumusan strategi pengamanan SPBE, BSSN tentunya harus memperhatikan visi dan misi SPBE yang tercantum di dalam Perpres No. 95 tahun 2018 tentang SPBE. Selain itu, BSSN juga perlu mengidentifikasi hambatan dan tantangan. Strategi alternatif juga perlu dirumuskan sebagai strategi cadangan apabila strategi pertama tidak dapat mencapai objektif yang telah ditentukan.

Tahap kedua merupakan implementasi strategi. BSSN yang telah diamanatkan melalui Perpres No. 95 SPBE sebagai penanggung jawab keamanan SPBE sewajibnya mengimplementasikan strategi yang telah dirumuskan. Namun, untuk menjamin implemetasi strategi tersebut, BSSN perlu menetapkan tujuan, menyusun kebijakan kebijakan, mengalokasikan sumber daya yang akan bekerja dalam melaksanakan strategi tersebut. Semuanya dapat dilakukan jika BSSN sebagai organisasi telah mengembangkan budaya yang mendukung strategi, meningkatkan efektivitas kerja dan menyiapkan susunan anggaran. Tahap ini tentunya menjadi tahap yang penting mengingat tahap ini merupakan *action stage* atau tahap aksi dimana strategi diterapkan.

Tahap terakhir yaitu evaluasi strategi. Tahap ini pada umumnya dilakukan oleh pimpinan lembaga yang dalam hal ini adalah Kepala BSSN untuk mengetahui pencapaian strategi pengamanan yang dilakukan oleh BSSN pada SPBE. Evaluasi strategi juga merupakan tahapan pemberian saran perbaikan pada strategi yang sedang diterapkan dengan tujuan untuk meningkatkan kualitas strategi tersebut kedepannya. Dalam konteks strategi pengamanan SPBE, BSSN melakukan evaluasi dengan tujuan untuk mengetahui dan menganalisis kesiapan pengamanan SPBE Nasional.

Selain dari aspek manajemen strategis, BSSN juga perlu menyusun strategi pengamanan dalam menghadapi ancaman siber terhadap SPBE karena adanya kerentanan yang masih cukup besar seperti yang telah dijelaskan sebelumnya. Oleh karena itu, analisa akan dikaji menggunakan teori strategi yang dikemukakan oleh Arthur F. Lykke dimana terdapat 3 (tiga) aspek dalam merumuskan sebuah strategi yaitu *ends, means* dan *ways*.

Ends merupakan sasaran (*objectives*) ataupun tujuan yang ingin dicapai dari strategi. Sedangkan *means* adalah segala sumber daya (*resources*) yang digunakan dan dikerahkan guna mencapai sasaran

utama dari strategi yang dijalankan. Lalu *ways* yang merupakan konsep-konsep (*concepts*), cara ataupun aksi yang digunakan dalam mencapai sasaran atau tujuan utama.[19]

Gambar 1. Rumus Strategi Arthur F. Lykke
Sumber: Arthur F. Lykke, 1998

Pertama adalah *means* atau sumber daya. Menurut Direktur Identifikasi Kerentanan dan Penilaian Risiko Pemerintah BSSN menyatakan bahwa pada pengamanan SPBE, Direktorat Proteksi Pemerintah dibawah Deputi 2 Bidang Proteksi merupakan *leading sector* dalam mewujudkan hal tersebut. Seperti yang diketahui, pembentukan unit kerja BSSN berdasarkan teori keamanan siber dimana pada saat menghadapi ancaman siber, tahap pertama yang dilakukan adalah identifikasi kerentanan pada sistem, lalu memproteksi sistem dan terakhir adalah memulihkan sistem yang terkena serangan. Artinya, dalam konteks BSSN setiap unit kerja, mulai dari Deputi 1 hingga Deputi 3 harus ikut menyusun regulasi keamanan SPBE. Sehingga *means* yang digunakan oleh BSSN dalam mengamankan SPBE baik pada aspek penyusunan regulasi dan aspek teknis adalah seluruh staf dan pejabat BSSN pada sektor pemerintah dari Deputi 1, Deputi 2 dan Deputi 3.

Kemudian *ways* atau cara. Sebelumnya telah dijelaskan beberapa konsep umum mengenai keamanan SPBE. Konsep-konsep tersebut merupakan cara BSSN dalam mengamankan SPBE yang dilaksanakan oleh setiap Deputi terkait. Sebagai contoh yaitu Deputi 1 Identifikasi dan Penilaian Risiko Pemerintah yang kemudian memiliki tugas mengamankan SPBE dengan cara melakukan penilaian kerentanan atau *security assessment* terhadap SPBE. Lalu Deputi 2 Proteksi yang mengamankan dengan menyusun regulasi mengenai manajemen pengamanan, standar teknis dan prosedur pengamanan SPBE, serta

[19] Arthur F. Lykke, Military Strategy: Theory and Application, (Pennsylvania: U.S. Army War College, 1998).

melakukan enkripsi pada data dan informasi yang ada di SPBE.

Kemudian Deputi 3 Penanggulangan dan Pemulihan Pemerintah yang membuat cara mitigasi dan *crisis management* pada saat terjadi insiden atau serangan siber terhadap SPBE. Masing-masing tentunya memiliki *ways* atau cara sesuai dengan tugas dan fungsinya. Yang terakhir adalah *ends* atau sasaran/tujuan.

Sasaran atau tujuan utama dari strategi pengamanan SPBE adalah untuk mewujudkan visi dan misi SPBE dalam menguatkan tata kelola SPBE khususnya keamanan informasi SPBE. Adapun tujuan khusus yang ingin dicapai yaitu melindungi aset yang berupa data dan informasi nasional sebagai bagian dari ketahanan dan keamanan SPBE.

Yang perlu diperhatikan adalah strategi ini hanya bisa berjalan jika arsitektur SPBE telah selesai disusun oleh Kemenpan RB, Kominfo dan BPPT. Strategi pengamanan BSSN juga membutuhkan kerjasama dan koordinasi dari setiap kementerian/lembaga dan pemerintah daerah yang menerapkan SPBE.

Pengamanan SPBE melalui strategi BSSN ini tentunya memiliki hambatan dan kendala dalam implementasinya. Penyusunan regulasi terkait keamanan SPBE masih sedang dikerjakan. Alhasil, strategi tentunya masih belum bisa diimplementasikan karena keterlambatan penyelesaian dari regulasi tersebut.

Adapun regulasi-regulasi yang sedang disusun berdasarkan tugas dan fungsi BSSN dalam Perpres 95 tahun 2018 yaitu Peraturan BSSN tentang Sistem Manajemen Pengamanan Informasi, Peraturan BSSN tentang Rencana Induk SPBE Bidang Keamanan, Peraturan BSSN tentang Standar Teknis dan Prosedur Pengamanan SPBE, dan Peraturan BSSN tentang Tata Cara Audit Keamanan SPBE. Penyusunan regulasi tersebut dikerjakan oleh Deputi 2 Bidang Proteksi Pemerintah yang memiliki tugas dalam menyusun kebijakan sistem keamanan informasi Pemerintah.

Jika mengacu pada tugas dan fungsi lembaga BSSN, penyusunan regulasi keamanan SPBE seharusnya tidak hanya dikerjakan oleh Deputi 2, tetapi juga oleh Deputi 1 dan Deputi 3 pada sektor pemerintah. Sehingga, menurut peneliti hambatan dalam penyusunan regulasi tersebut salah satunya adalah kekurangan sumber daya manusia (SDM) dimana hanya Deputi 2 Bidang Proteksi Pemerintah yang melakukan penyusunan

regulasi dan kebijakan. Oleh karena itu, perlunya pelibatan Deputi 1 dan Deputi 3 dalam penyusunan regulasi dan kebijakan, serta aspek teknis sehingga regulasi segera dirampungkan agar strategi pengamanan SPBE oleh BSSN dapat segera diterapkan atau diimplementasikan.

Selain dari aspek regulasi, pengamanan SPBE juga memiliki tantangan sebagai berikut:

1. ***Availability***

   Layanan SPBE umumnya membutuhkan ketersediaan data yang tinggi sehingga yang menjadi tantangan adalah menghadapi serangan terhadap ketersediaan data dan performa SPBE. Hal ini tentunya berkaitan dengan Pusat Data Nasional yang merupakan tanggung jawab dari Kominfo sehingga dalam hal ini BSSN perlu berkoordinasi dengan Kominfo dalam memberikan pertimbangan kelayakan keamanan dalam pembangunan Pusat Data Nasional.

2. ***Data Privacy/Confidentiality***

   Beberapa layanan SPBE mengelola data yang sifatnya pribadi dan bernilai. Tantangannya adalah bagaimana mengamankan data pribadi tersebut. Hal ini juga menjadi tanggung jawab Kominfo sebagai lembaga yang bertanggung jawab dalam integrasi dan interoperabilitas data, juga dalam pemanfaatan Pusat Data nasional. BSSN bertugas dalam menjaga kerahasiaan data para pernggguna SPBE.

3. ***Software Patching***

   Jumlah aplikasi SPBE yang dibagi menjadi 2 (dua) yaitu aplikasi umum dan aplikasi khusus kedepannya akan semakin bertambah jumlahnya yang tersebar di seluruh instansi pemerintah, sehingga tantangan yang akan dihadapi adalah bagaimana melakukan penambalan atau *patching* keamanan pada setiap aplikasi yang ada. Pada poin ketiga ini, yang diperlukan tidak hanya bagaimana cara melakukan *patching* pada setiap aplikasi, namun juga diperlukan orang-orang yang memiliki keahlian dalam melakukan *patching*. Sehingga kembali lagi bahwa SDM merupakan faktor penting dalam penerapan SPBE yang mana BSSN dapat berkoordinasi dengan Kemenpan RB selain dengan Kominfo.

4. ***Identity of Things***

   Belum adanya standar menjadi tantangan sendiri bagi identitas penyelenggara/pengguna SPBE dalam

melakukan otentikasi. Pada poin ini, BSSN perlu melakukan percepatan dalam penyelesaian penyusunan regulasi yang masih terhambat.

5. ***Logging***

   Mekanisme pencatatan *event-log* juga menjadi tantangan tersendiri bagi keamanan SPBE karena kedepannya akan banyak SPBE yang diterapkan oleh instansi pemerintah pusat dan pemerintah daerah. Sekali lagi bahwa SDM yang handal dalam pengamanan SPBE diperlukan dalam melakukan pencatatan terhadap *event-log*. Oleh karena itu, BSSN melalui Deputi 4 Direktorat Pengendalian Sumber Daya Manusia perlu berkoordinasi dengan Kemenpan RB dalam membangun SDM yang berkualitas pada bidang keamanan SPBE.

Kesimpulan dan Rekomendasi

Penerapan SPBE dari tahun 2003 hingga 2018, tepatnya sebelum Perpres No. 95 tahun 2018 tentang sistem pemerintahan berbasis elektronik diterbitkan masih mengalami beberapa hambatan dalam perkembangannya. Beberapa regulasi diterbitkan oleh pemerintah sejak tahun 2003, yaitu Inpres No.3 tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan *E-Government*, UU No. 14 tahun 2008 tentang Keterbukaan Informasi Publik, UU No. 25 tahun 2009 tentang Pelayanan Publik, UU 43 No. 2009 tentang Kearsipan dan UU No. 23 tahun 2014 Pemerintah Daerah.

Regulasi-regulasi tersebut dianggap belum dapat mengakselarasi penggunanaan *e-government* di Indonesia karena masih ditemukan beberapa hambatan. Pertama, luas wilayah Indonesia yang sangat luas sehingga menimbulkan gap terlalu tinggi dalam pembangunan infrastruktur. Ketimpangan terjadi antara wilayah Indonesia bagian barat dan timur sehingga tidak ada pemerataan. Masalah kedua adalah SDM. Kompetensi SDM dalam bidang SPBE masih juga masih menjadi kendala, terutama yang ada di daerah.

Yang ketiga adalah integrasi dan interoperabilitas data. Pembangunan *e-government* yang dilakukan oleh pemerintah pusat dan daerah dilaksanakan secara sendiri-sendiri atau *silo silo*, sehingga integrasi data untuk mewujudkan SPBE nasional menjadi sulit untuk dilakukan. Terakhir adalah pemborosan anggaran. Pembangunan aplikasi yang dilakukan oleh pemerintah pusat dan daerah terus dilakukan dan

tidak ada keseragaman arsitektur aplikasi sehingga pemerintah terus membuat aplikasi dan yang terjadi adalah pemborosan anggaran.

Pada perkembangannya, e-*government* yang sebelumnya hanya fokus pada situs dan aplikasi pemerintah mulai memfokuskan ke hal-hal lain seperti integrasi data dan keamanannya. Melalui Perpres 95/2018 tentang SPBE kemudian pemerintah membentuk Tim Koordinasi SPBE Nasional dengan tugas dan fungsi instansi masing-masing. BSSN merupakan badan siber nasional yang diberikan tanggung jawab dalam menyusun strategi pengamanan SPBE dari ancaman siber. Strategi pengamanan SPBE dilakukan untuk mewujudkan visi dan misi SPBE dalam menguatkan tata kelola SPBE khususnya keamanan informasi SPBE Nasional.

Namun, dalam strategi pengamanan SPBE oleh BSSN ditemukan beberapa hambatan dan kendala. Regulasi keamanan SPBE masih belum selesai dirampungkan oleh BSSN. Hingga pada tahun 2020 ini, regulasi-regulasi yang sedang disusun masih *on progress* berdasarkan Jaringan Dokumentasi dan Informasi Hukum BSSN. Oleh karena itu, perlu dilakukan percepatan kinerja agar strategi pengamanan tersebut segera diimplementasikan. Regulasi dan strategi pengamanan SPBE yang disusun oleh BSSN merupakan faktor penting dalam rangka kesiapan Indonesia dalam tata kelola sistem pemerintahan berbasis elektronik nasional menuju *i-government (integrated government).*

Berdasarkan kesimpulan diatas, peneliti kemudian akan memberikan rekomendasi bagi para pemangku kebijakan atau instansi terkait sebagai referensi dan masukan, yaitu:

1. Strategi yang telah diolah peneliti dapat menjadi strategi alternatif dalam pengamanan SPBE bagi BSSN.
2. Perlunya percepatan pada penyusunan regulasi keamanan SPBE yang dibuat oleh BSSN dengan melibatkan beberapa unit kerja dan tidak hanya fokus pada 1 (satu) unit kerja. Deputi 1, Deputi 2, dan Deputi 3 perlu ikut dalam hal itu agar dapat mengakselarasi penyusunan regulasi dan kebijakan terkait keamanan SPBE.
3. Perlunya kejelasan penyelenggaraan Infrastruktur Informasi Kritikal Nasional (IIKN) mengenai sektor pemerintah. Hal ini diperlukan mengingat SPBE yang merupakan sektor pemerintahan memiliki data dan informasi pribadi pengguna, baik

dari pemerintah, bisnis, dan masyarakat.

Daftar Pustaka

Buku

Creswell, John W.. (2010). *Research Design: Pendekatan Kualitatif, Kuantitatif dan Mixed*. Yogyakarta: PT. Pustaka Pelajar.

David, Fred R.. (2011). *Strategic Management: Concepts and Cases*. New Jersey: Prentice Hall.

Lykke Jr., Arthur F.. (1998). *Military Strategy: Theory and Application*. Pennsylvania: U.S. Army War College.

Miles, Matthew B., Huberman, A. Michael, dan Johnny Saldana. (2014). *Qualitative Data Analysis: A Methods Sourcebook*. Arizona: SAGE Publications, Inc.

Jurnal

Tan, W. & Subramaniam, R. (2005). "E-government: Implementation Policies and Best Practices from Singapore". *Electronic Government Strategies and Implementation*, hh. 305-324.

Zhao, Jensen J. dan Zhao, Sherry Y.. (2010). "Opportunities and Threats: A Security Assessment of State E-Government Websites". *Government Information Quarterly*, vol. 27(1), hh. 49-56.

Peraturan/Undang-Undang

Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik.

Website

Anggrahito. (2018). *Penerapan Vulnerability Assessment dan Penetration Test Bagi Pelaksanaan Audit Keamanan Informasi Sektor Pemerintah*. Retrieved from https://govcsirt.bssn.go.id/download/Penerapan-VA-dan-Pentest-bagi-Audit-Kaminfo-Sek.Pem-signed.pdf, diakses pada 10 Januari 2020.

Indrajit, Richardus Eko. (2013). *Evolusi Perkembangan Teknologi Informasi*. Retrieved from https://www.academia.edu/14351956/Evolusi_Perkembangan_Teknologi_Informasi, diakses pada 12 Juni 2019.

Indrajit, Richardus Eko. (2016). *Electronic Government*. Retrieved from https://www.academia.edu/30100450/Electronic_Government, diakses pada 9 Juni 2019.