Pemanfaatan IT-DRC sebagai Implementasi *Cyber Security* Pada Sistem Pemerintahan Berbasis Elektronik

Fauzia Gustarina Cempaka Timur [1], **Muh. Fachrul Febriansyah**[2], **Febyorita Amelia**[3]
[1,2,3] Universitas Pertahanan, Bogor, Indonesia

e-mail : **peperanganasimetris@gmail.com**

Abstrak— **Sistem Pemerintahan Berbasis Elektronik atau dikenal juga dengan *e-government* merupakan komitmen dan inisiatif pemerintah untuk meningkatkan hubungannya dengan masyarakat dan sektor bisnis melalui layanan yang efisien dan efektif menggunakan teknologi informasi dan komunikasi (TIK). Seiring dengan perkembangan layanan *e-government* yang melakukan pemanfaatan atas berbagai perangkat TIK, sistem *e-government* menjadi target potensial bagi para *hacker*. Karena intrusi yang dilakukan *hacker* terhadap sistem jaringan *e-government* dapat menganggu layanan pemerintah tersebut. Oleh sebab itu sistem informasi yang bersifat kritikal perlu di *backup* oleh *Information Technology – Disaster Recovery Center* (IT-DRC). Infrastruktur yang dimiliki oleh sistem *e-government* tidak akan lepas dari pembangunan *data center* sebagai *server* utama dan juga pembangunan IT-DRC sebagai suatu *backup* apabila *data center* utama mengalami gangguan. Penelitian ini membahas tentang IT-DRC yang ada di Kementerian Pertahanan lebih tepatnya mengenai IT-DRC sebagai backup dan *contingency planning* (CP) terhadap serangan siber. Tujuan dari penelitian ini adalah menganalisis strategi dan penanganan siber yang dilaksanakan dalam rangka implementasi konsep *cyber security* terutama melalui pemanfaatan IT-DRC. Metode penelitian yang digunakan dalam penelitian ini adalah Kualitatif dan teknik pengumpulan data primer menggunakan wawancara dan pengumpulan data sekunder dengan studi dokumen seperti laporan dan studi pustaka. Hasil penelitian ini memberikan rancangan kerangka dalam sistem pemerintahan berbasis elektronik di Indonesia, Peran dan penempatan IT-DRC serta rekomendasi dan kontribusi yang diberikan salah satunya berupa suatu standar operasional prosedur (SOP) penanganan siber secara *man-made* dan *non man-made* yang dapat diterapkan dalam kejadian yang tidak dapat diduga.**

Kata Kunci— E-government, IT-DRC, Cyber Security

I. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi 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. Selain perusahaan-perusahaan yang bergerak di bidang teknologi, internet 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 teknologi informasi dan komunikasi (TIK). *E-government* tidak hanya

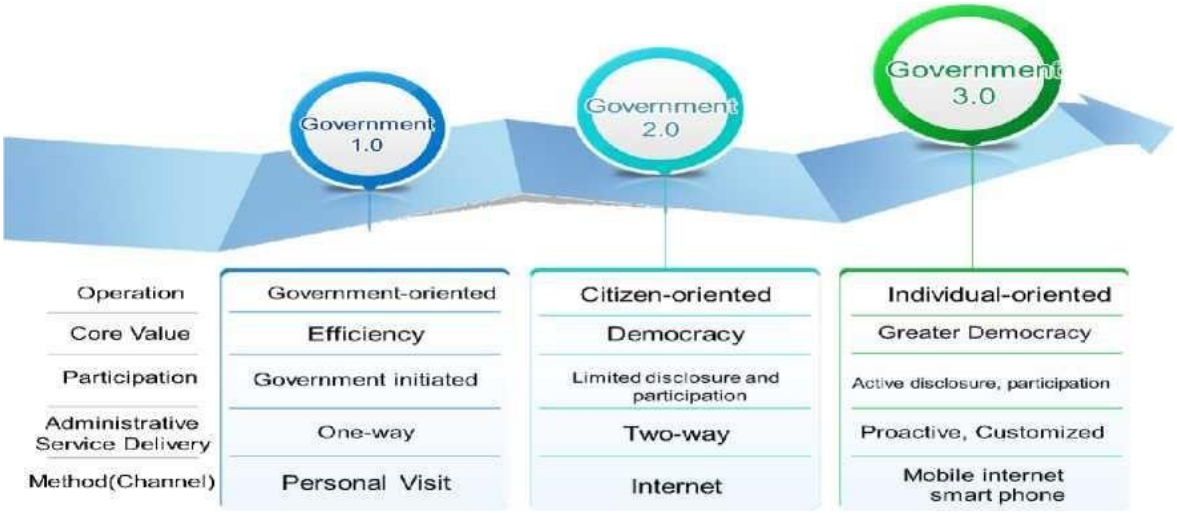
Received August 9th, 2019; Reviewed August 23rd, 2019; Accepted 4th, 2019

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 [1][2][3].

Sama halnya dengan teknologi informasi dan komunikasi, e-government juga telah mengalami perkembangan melalui beberapa era. Era pertama dikenal dengan *e-government* 1.0. Fase ini sendiri merupakan pertama kalinya penerapan *e-government* dilakukan oleh pemerintah di lingkungan pemerintah itu sendiri. *E-government* 1.0 lebih berfokus pada kebutuhan pemerintah sehingga hanya dijalankan oleh pemerintah. Tujuannya adalah untuk meningkatkan efisiensi kerja operasional para institusi atau lembaga di pemerintahan. Di Indonesia, salah satu contoh bentuk software yang digunakan oleh pemerintah adalah Sistem Informasi Keuangan Daerah. Salah satu ciri *e-government* 1.0 adalah sifatnya yang masih satu arah. Artinya, *e-government* hanya digunakan sebagai alat yang dapat meningkatkan efisiensi kerja sehingga pekerjaan lebih cepat [4].

Era kedua adalah *e-government* 2.0 yang mengacu pada kebijakan pemerintah dengan tujuan untuk memanfaatkan teknologi kolaboratif dan perangkat internet interaktif untuk menciptakan platform komputasi open-source dimana pemerintah, warga negara, dan sektor bisnis dapat meningkatkan transparansi dan efisiensi [5]. Sederhananya, *e-government* 2.0 adalah tentang bagaimana menempatkan pemerintahan di tangan warga [6]. Peran pemerintah adalah menyediakan data terbuka, layanan melalui situs atau *website* dan penggunaan *platform* sebagai infrastruktur [7]. Pada tahapan ini juga, *e-government* telah bersifat dua arah, nilai demokrasi mulai terlihat dan mulai adanya peningkatan pada interaksi pemerintah dengan masyarakat luas dan juga antar pemerintah sendiri.

Kemudian era terakhir yaitu era masa kini yang mengadaptasi model baru bernama *e-government* 3.0. Pada fase *e-government* 3.0, nilai-nilai demokrasi mulai dipraktikan secara luas. Jika sebelumnya praktik demokrasi hanya terbatas dimana warga negara hanya sekedar terlibat dengan pemerintah, maka pada fase ini warga negara akan sangat aktif dalam proses pemerintahan. Tiap individu dari masyarakat berpartisipasi atau menjadi proactive di dalam proses pemerintahan. Penggunaan internet 'konvensional' pun mulai berganti menjadi mobile internet smart phone, sehingga yang terjadi adalah teknologi yang diterapkan berorientasi individu atau personal [8].



Gambar 1. Fase–Fase *E-government* [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].

Seiring dengan perkembangan layanan *e-government* yang mulai memanfaatkan teknologi-teknologi masa depan tadi, sistem *e-government* menjadi target potensial bagi para penyerang siber yang biasa disebut sebagai hacker. Intrusi terhadap sistem jaringan *e-government* dapat menganggu layanan *e-government* kapan saja jika tidak diamankan dengan baik. Sebuah studi keamanan *e-government* pada tahun 2005 melaporkan bahwa 82% dari situs *e-government* 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) [10]. Indonesia sendiri tentunya memiliki kerentanan yang sama jika menggunakan perspektif bahwa tidak ada sistem yang aman.

Serangan siber semakin hari semakin bervariasi, dengan teknik kombinasi dari beberapa jenis serangan baik yang bersifat non man-made ataupun manmade, untuk menjaga keberlangsung bisnis suatu organisasi atau perusahaan, diperlukan sebuah fasilitas untuk menempatkan infrastruktur cadangan. Infrastruktur yang dimaksud adalah IT-DRC. Dengan adanya IT-DRC dalam sebuah organisasi, maka organisasi tersebut dapat segera mengalihkan sebagian atau bahkan keseluruhan operasional IT mereka kepada IT-DRC ketika terjadi bencana pada pusat data utama. *Disaster Recovery Center* atau bisa disebut sebagai IT-DRC (*Information Technology Disaster Recovery Center*) yang merupakan salah satu infrastruktur kritis (*Critical Infrastructure*) dalam IT.

IT-DRC disebutkan oleh Jamie Watters merupakan bagian dari *business continuity* yang berhubungan dengan melindungi dan memulihkan layanan kritikal IT [11]. IT-DRC berfungsi sebagai backup dari server pusat data utama apabila server pusat data utama mengalami gangguan yang dapat berupa gangguan secara *man-made* maupun *non man-made* sehingga IT-DRC harus di pantau kesiapannya setiap saat agar dapat berfungsi secara normal apabila terjadi gangguan. IT-DRC merupakan salah satu *critical infrastructure* dalam IT. NIST (*National Institute of Standart and Technology)* telah mengeluarkan tentang framework dalam memperkuat *critical infrastructure cybersecurity* pada April 2018. Tujuan utama pembuatan *framework* oleh NIST adalah untuk mengurangi dan mengelola resiko dari *cyber security* menjadi lebih baik.

II. LANDASAN TEORI

Landasan Teori dibutuhkan untuk menunjukkan hasil penelusuran pustaka yang membahas tema peneitian dan sebagai bukti bahwa tema penelitian yang diambil adalah masalah yang penting karena melibatkan perhatian banyak orang, sebagaimana ditunjukkan oleh kepustakaan yang dirujuk. Teori dan konsep ini akan digunakan sebagai landasan dan asumsi analisis yang kemudian akan digunakan dalam mengerjakan penelitian. Serangan siber semakin hari semakin bervariasi, dengan teknik kombinasi dari beberapa jenis serangan baik yang bersifat non man-made ataupun manmade, untuk menjaga keberlangsung bisnis suatu organisasi atau perusahaan, diperlukan sebuah fasilitas untuk menempatkan infrastruktur cadangan. Infrastruktur yang dimaksud adalah IT-DRC.

Dalam pembangunan infrastruktur kritis seperti sistem pemerintahan berbasis elekronik tidak akan lepas dari pembangunan *data center* sebagai *server* utama dan pembangunan IT-DRC sebagai suatu *backup* menjadi sangat penting apabila *data center* utama mengalami gangguan. Penelitian ini membahas tentang pemanfaatan IT-DRC pada sistem pemerintahan berbasis electronik di Indonesia yang mengimplementasikan konsep *cyber security*. Dalam pembahasan lebih lanjut akan dibahas konsep mengenai IT-DRC sebagai *backup* dan *contingency planning* (CP) terhadap serangan siber yang dapat terjadi pada sistem pemerintahan berbasis elekronik.

A. Cyber Security

Paul D. William menjelaskan bahwa keamanan adalah pengurangan dari ancaman yang membahayakan nilai-nilai yang dimiliki, hingga apabila tidak direspon dengan baik dapat mengancam keberlangsungan dari objek khusus yang dimaksud dimasa yang akan datang [12]. Penggunaan sistem internet yang hampir meliputi segala aspek kehidupan masyarakatnya membuat Amerika menjadi sasaran empuk sebagai target serangan siber. Tahun 2015, *Departement of Defense* Amerika Serikat mengeluarkan *cyber strategy* guna menjawab apa dan bagaimana mereka harus menjaga pertahanan Amerika Serikat di ranah siber. Prioritas mereka dalam keamanan siber yang merupakan prioritas dari pemerintahan Presiden Obama yaitu [13]:

1. Menjaga Sistem Informasi dan infrastruktur penting negara dari ancaman siber.
2. Meningkatkan kemampuan dalam mengidentifikasi dan melaporkan peristiwa-peristiwa siber agar dapat direspon secepat mungkin.
3. Membangun keamanan jaringan pemerintahan pusat dan menyusun target keamanan yang jelas dan menempatkan agen pemerintahan yang akuntabel.
4. Mengajak dunia untuk mempromosikan kebebasan internet dan membangun dukungan bagi ruang siber yang mudah dioperasikan, terbuka dan aman.
5. Membentuk kekuatan yang sangat memahami siber dan membangun kemitraan dengan *private sector*.

Adapun penjelasan lain mengenai keamanan siber atau *cyber security* yang dijelaskan oleh *International Telecommunications Union* (ITU), yaitu sebagai berikut:

> *"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment* [16]*."*

Mengacu pada penjelasan ITU diatas, maka bisa disimpulkan bahwa *cyber security* merupakan suatu usaha yang memanfaatkan alat, konsep, kebijakan dan teknologi dalam mengamankan sebuah lingkungan siber dan aset-aset pengguna. Lingkungan siber yang dimaksud dalam hal ini adalah sistem pemerintahan berbasis elektronik atau *e-government* yang menyangkut aset-aset pengguna di dalamnya, seperti pemerintah, masyarakat dan pihak bisnis.

B. E-Government

Menurut Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, Sistem Pemerintahan Berbasis Elektronik (SPBE) didefinisikan sebagai penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE (instansi pemerintah, aparatur sipil negara, pelaku bisnis, masyarakat dan pihak-pihak lainnya) [9]. Sistem Pemerintahan Berbasis Elektronik di dalam beberapa literatur lebih dikenal dengan istilah *e-government* pada umumnya yang menggambarkan suatu model ataupun sistem pemerintahan yang berbasis pada teknologi digital di dalam penyelenggaraannya seperti administrasi, pelayanan masyarakat/publik, keuangan, pajak dan lain-lain.

E-government merupakan adaptasi pemerintah dalam meningkatkan layanan publik dengan memanfaatkan teknologi informasi dan komunikasi yang bertujuan untuk memberikan layanan publik lebih transparan, efektif, dan efisien. Penyelenggaran *e-government* tentunya memberikan manfaat terhadap pelayanan publik yang diselenggarakan oleh pemerintah, baik itu pemerintah kepada masyarakat, pemerintah kepada pelaku bisnis dan antar institusi-institusi pemerintah (*inter-agency*). Al Gore dan Tony Blair dalam Indrajit menyebutkan setidaknya ada

enam manfaat yang dapat diperoleh oleh sebuah negara yang menerapkan sistem *e-government*, yaitu sebagai berikut [14]:

1. Meningkatkan efektivitas dan efisiensi kualitas pelayanan pemerintah kepada stakeholder yang terlibat ataupun pengguna e-government (masyarakat, pelaku bisnis dan industri).
2. Memberikan transparansi, kontrol dan akuntabilitas terhadap penyelenggaran pelayanan publik pemerintah dengan mengacu pada konsep good governance.
3. Menekan biaya administrasi dan interaksi yang dikeluarkan oleh pemerintah maupun beberapa stakeholder yang terlibat dalam aktivitasnya.
4. Menciptakan peluang bagi pemerintah sendiri untuk mendapatkan sumber pendapatan baru melalui kegiatan pelayanan publik dengan stakeholder yang memiliki kepentingan.
5. Menciptakan masyarakat yang lebih cepat, tepat dan tanggap dalam menjawab sebuah permasalahan dengan menyesuaikan perubahan global dan tren yang sedang terjadi.
6. Memberdayakan masyarakat dan stakeholder lainnya dalam proses pengambilan keputusan di berbagai kebijakan publik secara demokratis.

III. MODEL YANG DIUSULKAN

A. Pemanfaatan IT-DRC secara Umum

Information Technology - Disaster Recovery adalah bagian dari *business continuity* (kontinuitas bisnis) yang berhubungan dengan melindungi dan memulihkan layanan kritikal IT [11]. *Information Technology - Disaster Recovery* (IT-DRC) mengacu kepada cara untuk melindungi sistem dari bencana and proses yang diikuti untuk memulihkannya dari bencana. *Disaster recovery* dirancang untuk mendahului kontinuitas bisnis dan merupakan sesuatu yang mulai dipikirkan oleh orang IT segera setelah komputer digunakan untuk aplikasi komersil. Hal ini dilakukan karena organisasi atau perusahaan semakin bergantung kepada sistem dan mereka perlu menemukan cara untuk mengembalikan dan menjalankan bisnis jika komputer mati atau menemui kendala. Jamie Watters mengkategorikan beberapa solusi dalam *disaster recovery* yang didorong oleh persyaratan bisnis yaitu *recovery time objective* (RTO) dan *recovery point objective* (RPO).

Jamie Watters mengkategorikan mengenai solusi dalam *disaster recovery* yang didorong oleh persyaratan bisnis yaitu *Hot standby, Warm recovery, Cold Recovery, Resilience* dan *Mobile recovery* [11] sehingga IT-DRC dapat ditingkatkan perannya sebagai suatu *contingency planning* (CP) yang dapat diterapkan apabila terjadi kejadian yang tidak terduga-duga. Kelima tahapan *disaster recovery* tersebut memfokuskan pada dua aspek, yaitu *recovery time objective* (RTO) dan *recovery point objective* (RPO). *Recovery time objective* sendiri merupakan aksi dalam menentukan seberapa cepat suatu sistem harus dipulihkan setelah gagal akibat adanya insiden atau bencana. Sedangkan *recovery point objective* bertujuan untuk menentukan jumlah maksimum kehilangan data. Dengan kata lain, RPO memberi tahu pengguna seberapa jauh pengguna dapat mengembalikan data saat memulihkan suatu sistem, yang dalam hal ini adalah data dan informasi dari sistem pemerintahan berbasis elektronik.

Seperti yang telah disebutkan sebelumnya, bahwa terdapat lima aspek dalam *disaster recovery* sebagai solusi ketika sebuah sistem mengalami insiden atau bencana. Berikut pengertian lebih dalam mengenai kelima aspek tersebut [11]:

1. *Hot Standby*
   Hot standby pada dasarnya membuat sistem yang sama persis atau menduplikasi dengan sistem yang sedang dijalankan saat ini, mulai dari perangkat keras, perangkat lunak, hingga data yang ada.
2. *Warm Recovery*
   Sama halnya dengan *hot standby*, *warm recovery* merupakan pemulihan yang memanfaatkan dua sistem namun sistem atau pusat data kedua tidak persis sama dengan

sistem pertama atau yang sedang berjalan. Sistem kedua berfungsi untuk membantu memulihkan jaringan dan data pada sistem pertama melalui *remote* dari jarak jauh.

3. *Cold Recovery*
   Berbeda dengan *hot standby* dan *warm recovery*, *cold recovery* tidak memiliki sistem kedua yang siap berjalan dan digunakan ketika insiden terjadi. Sehingga, *cold recovery* cenderung menggunakan pihak ketiga dalam pemulihan data. Hal terebut tentunya dapat mengurangi biaya, namun pemilik sistem akan kehilangan fleksibilitas dan control pada saat uji ulang sistem.

4. *Resilience*
   Resilience bukan bagian dari *disaster recovery*. Sebaliknya, *resilience* adalah cara untuk menghindari kebutuhan akan *disaster recovery* dalam sejumlah scenario. Dengan membangun sebuah sistem pemerintahan berbasis elektronik yang kuat dengan tidak memiliki kerentanan, maka insiden atau bencana dapat dihindari sehingga *disaster recovery* tidak dibutuhkan.

5. *Mobile Recovery*
   Mobile recovery merupakan tindakan pemulihan yang tidak mengandalkan sistem atau pusat data tradisional seperti halnya *hot standby*, *warm recovery* dan *cold recovery*. Data pada *mobile recovery* cenderung dipulihkan dan dipindahkan pada lokasi yang diinginkan oleh pengguna.

Gambar 2. Pemanfaatan *Information Technology Disaster Recovery* sebagai bagian dari Sistem *Cyber Security*

Standarisasi dalam membangun IT-DRC adalah ISO 27001 tentang sistem manajemen keamanan informasi. Selain itu, untuk membangun fisik gedung yang akan dipakai sebagai bangunan IT-DRC juga harus memperhatikan konsep design pembangunan *data center*. Konsep design pembangunan *data center* sesuai standar yaitu [14]:

1. Penentuan lokasi *data center*. Kriteria penentuan lokasi *data center* yaitu diluar jalur gempa bumi, banjir dan tsunami, minimal 30 KM dari pusat aktivitas organisasi dan maksimal 50 KM untuk mengurangi resiko *data loss*, jauh dari jalur penerbangan pesawat dan mudah diakses.
2. Desain dan arsitektur gedung/ruang *data center*. Hal-hal yang perlu diperhatikan untuk membangun *Disaster Recovery Center* yaitu : (a) Sistem *power supply*: pPasokan listrik dari 2 sumber berbeda, genset dengan pasokan listrik besar, *redudant* UPS, dan *battery backup*. (b) Sistem lingkungan: Sistem HVAC N+1 *redudant* untuk menjamin suhu, aliran udara dan kelembaban, *fire suppression* dan EMS. (c) *Connectivity*: Media akses FO, *Microwave* dan Satelit (d) *Security*: Sistem keamanan berlapis 24x7, CCTV, pintu akses masuk dengan pemindai biometrik
3. Luas ruangan, pemilihan jenis *rack server*, dan pengaturan kabel. Dalam membangun sebuah bangunan IT-DRC maka perlu bertahan dari gempa bumi yang terstandarisasi SNI No.03-1726-2003, tanah longsor dan serangan sambaran petir. Hal mengenai penempatan IT-DRC ini perlu dianalisa kembali.

IV. IMPLEMENTASI MODEL DAN PEMBAHASAN

Proteksi wajib dilakukan melalui implementasi konsep *cyber security* yang tepat 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. *E-government* memiliki empat tipe relasi yaitu, *government to citizens* (G to C), *government to businesses* (G to B), *government to governments* (G to G), dan *government to employees* (G to E) [15].

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 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 proteksi yang dilakukan melalui IT-DRC pada sistem pemerintahan berbasis elektronik.

Penentuan lokasi IT-DRC minimal 30 KM dan maksimal 50KM dari pusat organisasi. Hal ini diperlukan untuk menghindari gangguan transmisi data yang dapat menyebabkan data loss. Lalu lokasi IT-DRC harus jauh dari jalur penerbangan pesawat dan mudah diakses. Selain penentuan lokasi fisik, hal lain yang perlu diperhatikan adalah mengenai sistem pendukung IT-DRC seperti sistem catu daya sebagai pemasok aliran listrik. Idealnya diperlukan dua atau lebih sumber pemasok daya yang berbeda yang menyediakan aliran listrik IT-DRC. Selain itu diperlukan Generator dengan pasokan listrik yang besar, *Redudan*t UPS, *Battery Backup* yang berfungsi untuk menjamin ketersedian aliran listrik apabila penyedia aliran listrik utama mengalami gangguan.

Selain itu sistem lingkungan yang terintegrasi sangat dibutuhkan untuk memantau kondisi lingkungan IT-DRC seperti pemantauan suhu, aliran udara, kelembapan, *fire suppression* dan EMS yang mengatur seluruh sistem lingkungan. Hal terakhir yang perlu diperhatikan adalah mengenai sistem konektivitas. Sistem konektivitas merupakan hal yang paling rentan dalam penjaminan keberlangsungan IT-DRC. Oleh sebab itu, diperlukan sistem konektivitas yang lebih dari satu untuk menjamin transfer data dari pusat data utama ke IT-DRC tidak terkendala.

V. KESIMPULAN

Teknologi informasi dan komunikasi (TIK) yang merupakan sarana yang digunakan dalam membangun sebuah sistem *e-government*. pemerintah selaku aktor yang menjalankan, menyelenggarakan dan mengadaptasi kegiatan *e-government*. *E-government* menuntut penggunaan teknologi informasi dan komunikasi yang dilakukan oleh pemerintah dalam memberikan layanan publik dengan akses yang cepat, tepat dan efisien kepada masyarakat dan para pelaku bisnis. Penyelenggaran *e-government* tentunya memberikan manfaat terhadap pelayanan publik yang diselenggarakan oleh pemerintah, baik itu pemerintah kepada masyarakat, pemerintah kepada pelaku bisnis dan antar institusi-institusi pemerintah.Dalam memanfaatkan sistem *cyber security*, penanggulangan manajemen resiko *e-government* lebih tepat mengimplementasikan manajemen resiko pada *e-government* melalui beberapa tahapan. Pertama mendeteksi kerentanan sistem, kedua analisis resiko yang kemungkinan terjadi kemudian membuat rencana dan langkah kedepan, dan terakhir manajemen resiko harus menyesuaikan dengan perubahan lingkungandan buat rencana pemulihan. Salah satu pemanfaatan *cyber security* tersebut adalah melalui IT-DRC. IT-DRC merupakan infrastruktur

server yang bertugas untuk melakukan *backup* pusat data utama apabila pusat data utama mengalami gangguan atau *failure*. IT-DRC dapat ditingkatkan perannya sebagai suatu *contingency planning* yang dapat diterapkan apabila terjadi kejadian yang tidak terduga.

DAFTAR PUSTAKA

[1] Weiling Ke & Kwok Kee Wei, "Successful e-government in Singapore*",* in *Communications of the ACM,* 2004, vol. 47, no. 6, pp. 95–99.

[2] Chee-Wee Tan, Shan L. Pan, and Eric Tze Kuan Lim, "Managing Stakeholder Interests in e-Government Implementation: Lessons Learnt from a Singapore e-Government Project," in *Journal of Global Information Management, 2005, vol.* 13, no. 1, pp. 31-53.

[3] Darrell M. West, "Assessing E-government: The Internet, democracy, and service delivery by state and federal government", *The Genesis Institute*, 2000, pp. 1-29. Retrieved from http://www.insidepolitics.org/egovtreport00.html

[4] Ignatius Novianto Hariwibowo, Memahami Evolusi E-Government, 2019, Retrieved from https://opini.harianjogja.com/read/2019/01/24/543/967190/opini-memahami-evolusi-e-government

[5] Tim O'Reilly, *What is Web 2.0: Design Pattern and Business Models for the Next Generation of Software*. Boston: O'Reilly Media, 2009.

[6] Logan Harper, *Gov 2.0 Rises to the Next Level: Open Data in n Action*, 2013, Retrieved from http://opensource.com/government/13/3/future-gov-20

[7] Anne Howard, *Connecting with Communities: How Local Government Is Using Social Media to Engage with Citizens*. Canberra: ANZSOG Institute for Governance at the University of Canberra and Australian Centre of Excellence for Local Government, 2012.

[8] June-Suh Cho, "Evolution of e-government: Transparency, competency, and serviceoriented government with Korean government 3.0", in *Journal of Business and Retail Management Research*, 2017, vol. 12, issue 1, pp. 62-68.

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

[10] Jensen J. Zhao and Sherry Y. Zhao, "Opportunities and Threats: A Security Assessment of State E-government Websites", in *Government Information Quarterly*, 2010, vol. 27, no. 1, pp. 49-56.

[11] Jamie Watters, *Disaster Recovery, Crisis Response, & Business Contibuity: A Management Desk Reference*. New York: Apress Media, 2014.

[12] Paul D Williams, *Security Studies: An Introduction*. USA: Routedge, 2008.

[13] *Dewi Triwahyuni dan Tine Agustin Wulandari, "*Strategi Keamanan Cyber Amerika Serikat*",* in *Jurnal Ilmu Politik dan Komunikasi*, vol. 6, no. 1, 2016, pp. 107-118.

[14] Konsep Design Pembangunan Data Center Sesuai Standard. Teknologi Data Center, 2016, Retrieved from https://mobnasesemka.com/design-pembangunan-data-center/

[15] Richardus Eko Indrajit, *Konsep dan Strategi: Electronic Government*. Yogyakarta: ANDI, 2016.

[16] International Telecommunication Union, *Introduction to Security Cyberspace, Cybercrime and Cybersecurity*, 2008, Retrieved from https://www.itu.int/rec/T-REC-X.1205-200804-I

Fauzia Gustarina Cempaka Timur S.IP., M.Si (Han) saat ini merupakan dosen di Program Studi Peperangan Asimetris, Universitas Pertahanan dan di Program Studi Hubungan Internasional *International University Liaison Indonesia*. Ia meraih gelar Magister Ilmu Pertahanan dari Universitas Pertahanan di Prodi Peperangan Asimetris dan gelar sarjana di bidang Hubungan Internasional dari Universitas Gadjah Mada, Yogyakarta serta untuk kedua gelar tersebut mendapatkan predikat *Cum Laude*. Saat ini ia tengah menyelesaikan Pendidikan Doktoral di bidang Hubungan Internasional di Universitas Padjajaran, Bandung melalui disertasinya yang mengambil tema tentang Kontra-Terorisme di Asia Tenggara. Penelitian kolaborasi ini dibuat bersama dengan Muh. Fachrul Febriansyah, S.H.Int. (Mahasiswa S-2 Universitas Pertahanan) dan Febyorita Amelia, S.Psi (Mahasiswa S-2 Universitas Pertahanan).