METODOLOGI PENILAIAN KERENTANAN PADA INFRASTRUKTUR KRITIKAL NASIONAL

I Made Mustika Kerta Astawa
Badan Siber dan Sandi Negara
Ragunan, Jakarta Selatan
Kadek19_kaptainboy@yahoo.com

Abstrak— Sistem Infrastruktur Kritikal Nasional seperti listrik, telekomunikasi, transportasi, utilitas air, distribusi makanan, perumahan dan tempat tinggal, kesehatan masyarakat, keuangan, perbankan dan lain sebagainya merupakan fondasi kebutuhan masyarakat modern. Pemerintah Indonesia telah sangat sadar akan pentingnya infrastruktur kritikal nasional terhadap ekonomi bangsa dan kualitas hidup masyarakat. Di era digital, Ketergantungan masyarakat pada sistem infrastruktur kritikal nasional menjadikannya sasaran serangan yang sangat menarik khususnya serangan siber. Untuk memahami kerentanan dan acaman pada infrastruktur kritikal nasional, sangat penting untuk memulai dari metodologi yang tepat dalam melakukan penilaian kerentanan dan penilaian risiko. Makalah ini mengusulkan dan menjelaskan metodologi umum dalam melakukan penilaian kerentanan pada infrastruktur kritikal nasional. Metodologi ini dirancang untuk menjadi framework komprehensif dalam hal antisipasi adanya gangguan dan acaman siber. Sementara penekanannya adalah pada penilaian kerentanan, dimana hasilnya memberikan banyak bahan penting dari penilaian risiko.

***Kata kunci*— Penilaian Kerentanan, Infrastruktur Kritikal Nasional**

I. PENDAHULUAN

Bagian Pendahuluan membahas latar belakang masalah, Pada tahun 2003, Departemen Keamanan Dalam Negeri Amerika Serikat mengeluarkan dokumen strategi nasional untuk perlindungan infrastruktur nasional baik secara fisik maupun siber yang menyerukan penilaian kerentanan terhadap sistem infrastruktur kritikal nasional (IKN). Strategi yang dijelaskan pada dokumen tersebut tentang bagaimana mengidentifikasi dan mengurangi kerentanan sistem. Sebagai langkah pertama, dokumen strategi meminta penyedia layanan IKN untuk menilai kerentanan aset mereka.

Makalah ini menguraikan metodologi umum, yang dapat digunakan untuk penilaian kerentanan pada IKN. Meskipun metodologi ini berfokus pada fasilitas organisasi (stakeholder terkait di sektor IKN), namun hasilnya dapat digunakan dalam penilaian sektor skala yang lebih besar untuk menentukan peringkat fasilitas infrastruktur, sehingga memberikan dasar untuk menentukan prioritas dan alokasi sumber daya. Metodologi penilaian ini bersifat komprehensif karena membahas berbagai ancaman, termasuk fisik dan siber, terhadap keseluruhan fasilitas dan sistem IKN [1].

Metodologi ini mengacu pada penilaian kerentanan di sektor IKN yaitu sektor telekomunikasi yang dilakukan oleh *Institute of Infrastructure and Information Assurance* di *James Madison University*. Metodologi ini berfokus pada penilaian kerentanan dalam konteks penilaian risiko pada sektor IKN. Selain itu, metodologi ini dapat digunakan oleh stakeholder IKN serta tim penilai pihak ketiga (termasuk Badan Siber dan Sandi Negara dalam mengidentifikasi sektor IKN). Kemampuan stakeholder IKN untuk menilai diri mereka sendiri sangat penting mengingat ratusan ribu fasilitas dan sistem IKN di Indonesia yang perlu dinilai.

II. LITERATUR REVIEW

Hampir setiap Negara di Dunia memiliki pandangan yang berbeda terkait dengan Infrastruktur Kritikal Nasional (IKN) dan Infrastruktur Informasi Kritikal Nasional (IIKN). Berikut merupakan literatur review :

A. Definisi dan Kriteria Umum Informasi Kritikal Nasional

Berikut merupakan beberapa pengertian infrastruktur kritikal yang diperoleh dari beberapa referensi [2]:

a. *International Organization for Standardization* (ISO:2013) mendefinisikan *critical infrastructure* sebagai fasilitas atau layanan yang penting dalam menunjang kehidupan masyarakat dan perekonomian secara keseluruhan, kegagalan atau tidak berfungsinya IKN dapat menyebabkan terhentinya pasokan, mengakibatkan terganggunya keamanan publik dan memiliki dampak kerugian yang meluas lainnya.

b. *International Telecommunication Union* (ITU:2008) menyatakan bahwa *critical infrastructure* merupakan sistem utama, layanan, fasilitas dan fungsi yang apabila terjadi gangguan atau hancurnya IKN akan memiliki dampak yang dapat melemahkan sektor kesehatan, perdagangan dan perekonomian, mengancam keselamatan publik serta keamanan nasional atau kombinasi dari semua ini.

c. Negara Australia mendefinisikan *critical infrastruture* sebagai fasilitas fisik, proses suplai, teknologi informasi dan jaringan komunikasi, dimana jika terjadi kehancuran, terdegradasi atau tidak tersedia untuk jangka waktu lama, akan berdampak secara signifikan pada kesejahteraan sosial

atau ekonomi negara atau mempengaruhi kemampuan Australia untuk melakukan pertahanan nasional dan memastikan keamanan nasional.

d. Negara Victoria mendefinisikan bahwa komponen Infrastruktur Kritis ICT disebut sebagai bagian dari IKN, dimana Infrastructure Critical Cyber/ ICT merupakan infrastruktur siber yang penting bagi layanan vital untuk keselamatan publik, stabilitas ekonomi, keamanan nasional, stabilitas internasional dan untuk keberlanjutan dan pemulihan di dunia siber.

e. Negara Amerika Serikat mendefinisikan critical infrastructure adalah sistem, aset dan jaringan, baik fisik atau virtual yang sangat penting bagi Amerika Serikat yang apabila terjadi ketidakmampuan atau kehancuran sistem, aset dan jaringan tersebut memiliki dampak lemahnya keamanan, keamanan ekonomi nasional, kesehatan atau keselamatan publik, atau kombinasi dari dampak-dampak tersebut.

f. Negara Inggris menyebutkan bahwa IIKN terdiri dari aset, layanan, dan sistem yang mendukung kehidupan ekonomi, politik, dan sosial Inggris yang sedemikian kerugiannya: 1) menyebabkan hilangnya nyawa dalam jumlah besar; 2) memiliki dampak serius pada ekonomi nasional; 3) memiliki konsekuensi sosial berat lainnya bagi masyarakat; atau 3) menjadi perhatian langsung kepada pemerintah nasional.

Berdasarkan pengertian yang diperoleh dari beberapa referensi di atas, dapat digeneralisasikan bahwa infrastruktur kritikal merupakan sistem, layanan atau fasilitas yang menunjang kehidupan masyarakat secara keseluruhan, yang apabila terjadi gangguan atau tidak berfungsinya infrastruktur kritikal maka dapat menyebabkan dampak yang sangat signifikan bagi ketahanan, keamanan, perekonomian negara, kesehatan dan keselamatan masyarakat, atau dampak lain yang dianggap vital bagi suatu negara.

B. Definisi dan Kriteria Umum IIKN

Berikut merupakan beberapa pengertian infrastruktur informasi kritikal yang diperoleh dari beberapa referensi [2]:

1. *Organisation for Economic Co-Operation and Development* (OECD) mendefinisikan IIKN adalah sekumpulan sistem informasi yang saling berhubungan dan sistem jaringan informasi (komputerisasi), dimana apabila terjadi gangguan atau kehancuran pada sistem tersebut akan memiliki dampak serius pada kesehatan, keselamatan, keamanan, atau kesejahteraan ekonomi masyarakat, atau pada fungsi efektif pemerintah atau perekonomian.
2. *Negara* Brasil mendefiniskan bahwa IIKN adalah bagian dari aset informasi yang secara langsung mempengaruhi pencapaian dan kelangsungan misi negara dan keselamatan masyarakat.
3. *Negara* Inggris menyebutkan bahwa IIKN dapat merujuk ke sistem Teknologi Informasi apapun yang mendukung aset dan layanan utama dalam infrastruktur nasional
4. Negara Malaysia mendefinisikan bahwa IIKN adalah aset (real & virtual), sistem dan fungsi yang esensial bagi Negara dimana jika terjadi kerusakan atau kehancuran dari aset, sistem dan fungsi tersebut akan memiliki dampak yang menghancurkan terhadap pertahanan dan keamanan Nasional, kekuatan ekonomi nasional, citra nasional, kemampuan pemerintah, kesehatan masyarakat dan keselamatan.

Berdasarkan pengertian yang diperoleh dari beberapa referensi di atas, dapat digeneralisasikan bahwa infrastruktur informasi kritikal merupakan sekumpulan aset (real dan virtual), sistem informasi yang saling berhubungan dan sistem jaringan informasi/komputerisasi yang esensial bagi negara guna mendukung aset dan layanan utama dalam infastruktur nasional, yang apabila terjadi gangguan atau tidak berfungsinya infrastruktur informasi kritikal maka dapat menyebabkan dampak yang sangat signifikan bagi ketahanan, keamanan, perekonomian negara, kesehatan dan keselamatan masyarakat, atau dampak lain yang dianggap vital bagi suatu negara.

III. USULAN PENILAIAN

Penentuan IKN berbeda-beda tergantung pada cara penilaian di negara tersebut. Berikut merupakan usulan penilaian yang dapat dilakukan untuk menentukan kriteria IKN di Indonesia yaitu dengan Mekanisme Penilaian Kerentanan dalam Konteks Penilaian Risiko.

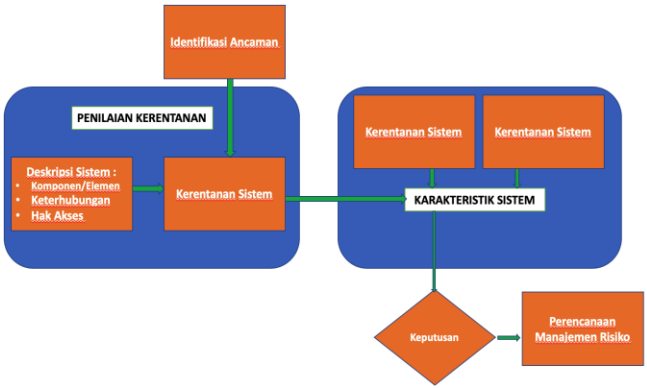
Penilaian kerentanan adalah subset penting dari proses penilaian risiko (lihat gambar 1). Penilaian kerentanan dapat dilakukan dengan melihat elemen-elemen sistem dan tata letak serta kemungkinan kegagalannya berdasarkan serangkaian ancaman atau kerawanan yang dapat terjadi. Penilaian kerentanan menjawab pertanyaan dasar, apa dampak risiko yang ditimbulkan jika sistem terkena ancaman dan serangan?. Sehingga masing-masing pemilik sistem (stakeholder) dapat melakukan penilaian kerentanan [2].

Proses penilaian risiko menggunakan hasil penilaian kerentanan untuk menjawab pertanyaan tambahan berikut:

1. Berdasarkan kerentanan yang diidentifikasi, apa dimungkinkan menyebabkan terjadinya kegagalan sistem?
2. Apa konsekuensi dari kegagalan tersebut (mis. Biaya, nyawa)?
3. Apakah konsekuensi ini dapat diterima?

Meskipun risiko sering dihitung menggunakan persamaan kemungkinan dan biaya, penilaian risiko berakhir dengan penilaian pemangku kepentingan terhadap risiko kelangsungan proses bisnis dan layanannya. Penentuan risiko dimulai dengan hasil penilaian kerentanan dan menambahkan pertimbangan kemungkinan ancaman ditambah dengan konsekuensi ekonomi, politik dan sosial dari kegagalan sistem IKN [3]. Akhir dari proses penilaian risiko adalah keputusan mengenai apakah akan mengambil tindakan atau tidak berdasarkan pada penerimaan risiko yang diidentifikasi.

[a]Identify applicable sponsor/s here. If no sponsors, delete this text box (*sponsors)*.



Gambar 1. Proses Penilaian Risiko

Metodologi penilaian kerentanan memiliki tujuan sebagai berikut:

1. Memahami sistem dan fasilitas pendukungnya di organisasi
2. Identifikasi kerentanan yang dapat mengancam sistem infrastruktur kritikal
3. Memahami desain dan operasional sistem untuk menentukan kerentanan dan kemungkinan kegagalan
4. Jika memungkinkan, identifikasi konsekuensi dari kegagalan sistem dalam hal waktu henti, efek pada orang, dan setiap efek *cascading* pada sistem dan organisasi lain. (Walaupun analisis biaya kegagalan bukan merupakan bagian eksplisit dari penilaian kerentanan, informasi tersebut dapat mengalir dari peninjauan kejadian sebelumnya.)
5. Merekomendasikan perbaikan sistem untuk mengurangi kerentanan

Tujuan penilaian kerentanan diatas dapat dicapai dengan proses/langkah sebagai berikut (tahapan tidak harus dilakukan secara berurutan):

1. Identifikasi Ancaman/Kerawanan: Penilaian kerentanan akan didorong oleh serangkaian ancaman dan kerawanan yang dapat mempengaruhi sistem IKN. Ancaman mengacu pada seluruh kemungkinan termasuk serangan siber dan fisik atau sabotase. Kerawanan mengacu pada bencana alam atau kecelakaan normal yang mungkin terjadi secara acak. Kemungkinan dan tingkat keparahan juga harus diidentifikasi untuk setiap jenis ancaman dan kerawanan yang dianggap layak diperhatikan. Misalkan saja serangan komputer mungkin terjadi setiap hari (kemungkinan) dan mempengaruhi 10 komputer (tingkat keparahan). Perlu menjadi perhatian bahwa segala bentuk ancaman dan kerawanan yang telah terjadi di masa lalu pada IKN harus ada dalam daftar.

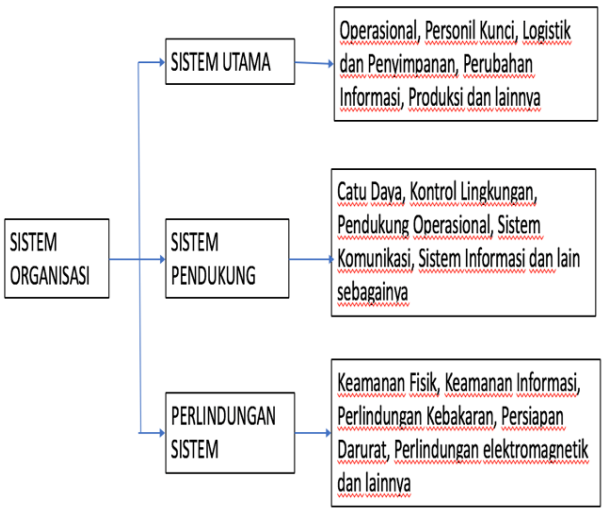
Kantor penegakan hukum dan FBI setempat dapat membantu mengidentifikasi kegiatan dan organisasi yang bermusuhan yang dapat mengancam fasilitas infrastruktur. Ini juga merupakan latihan yang berguna untuk mempertimbangkan alasan mengapa fasilitas Anda mungkin ditargetkan.

Dalam melakukan identifikasi kerentanan, pemangku kepentingan perlu menyediakan forum yang berguna untuk menggambarkan, mendiskusikan, dan melawan kemungkinan ancaman yang dapat terjadi. Contoh Daftar ancaman dan kerentanan yang dapat terjadi seperti pada Table 1. Namun, tidak semua ancaman dan kerentan yang terdaftar akan berkaitan di semua sektor IKN.

TABEL I. CONTOH ANCAMAN/KERENTANAN

Ancaman	Elemen Khusus
	Isu Internal
Kecelakaan	Kebakaran, Kontaminasi, kegagaglan terstruktur
Aktivitas Kriminal	Pembakaran, Serangan Personal, Perusakan
Sabotase	Merusak, Membakar, Manipulasi Data, penyusupan malware dan Pencurian
	Isu Eksternal
Terorisme	Paksaan, Teror, Kejadian terstruktur
Perang Informasi	Virus, Trojan, Perubahan Data
Kejadian Alam	Gempa Bumi, Angin Topan, Banjir, Kebakaran

2. Identifikasi Sistem : Karakterisasi IKN dimulai dengan identifikasi sistem dan fungsi utama yang diperlukan untuk mendukung layanan dan proses bisnis pemangku kepentingan. Sebagai contoh, sistem pabrik untuk memproduksi dan mengirimkan sejumlah barang tertentu per bulan. Fungsi pendukung dapat mencakup jalur produksi otomatis, bagian pengiriman dan penerimaan, dan basis data komputer dan sistem SCADA yang diperlukan untuk menyimpan catatan dan mengontrol proses pembuatan.
3. Identifikasi Sistem Pendukung : Berdasarkan pada sistem utama yang diperlukan untuk melakukan fungsi utama, perlu juga untuk mengidentifikasi sistem pendukung yang menunjang kegiatan. Misalnya sistem pabrik sebagai fungsi utama untuk memproduksi. Namun, yang tak kalah penting dari sudut pandang operasi sistem adalah sistem pendukung yang umum untuk semua fasilitas seperti tenaga listrik, telekomunikasi, pasokan air, jaringan komputer, sistem pengawasan dan sistem akuisisi data (SCADA), sistem pemanas-ventilasi-pendingin udara (HVAC) dan sistem keamanan. Sistem pendukung ini seringkali lebih rentan daripada sistem utama karena kurangnya perhatian. Taksonomi sistem di dalam sistem dicantumkan pada Gambar 2. Ini umum untuk banyak jenis sistem. Hal ini sangat bermanfaat untuk penilaian kerentanan pada keseluruhan fungsi utama baik dari sistem utama maupun sistem pendukung.



Gambar 2. Taksonomi Sistem

4. Interkoneksi Elemen Sistem Kritikal dan Saling Ketergantungan: Setelah mengidentifikasi sistem yang diperlukan untuk melakukan fungsi utama, penting untuk mengetahui dan menelusuri hubungan antara sistem yang kritikal. Hasilnya akan menjadi diagram fungsional sistem yang menggambarkan bagaimana sistem kritikal saling berhubungan. Dari skema interkoneksi sistem kadang-kadang berguna untuk mengembangkan representasi titik kesalahan dari ketergantungan logis sistem utama pada sistem pendukung. Memahami saling ketergantungan sistem memungkinkan evaluasi kegagalan berjenjang di mana kegagalan satu sistem dapat memiliki efek hilir pada satu atau lebih sistem tambahan. Diagram fungsional dan kesalahan sistem adalah dasar untuk analisis komputer terhadap respons ancaman sistem. Pertimbangan penting yang terkait adalah apakah sistem kritikal memiliki sistem cadangan, atau penggantian suku cadang yang tersedia jika sistem kritikal tersebut tidak berfungsi.
5. Rekonstitusi Sistem: Interkoneksi dan interdependensi sistem fisik/logis hanyalah satu bagian dari persamaan. Durasi pemadaman sistem kritikal secara keseluruhan perlu dievaluasi untuk ancaman dan kerawanan yang menjadi perhatian. Ini melibatkan pemahaman faktor waktu yang terkait dengan kerentanan sistem kritikal. Yaitu, jika suatu sistem gagal, berapa lama untuk memperbaiki atau menggantinya? Faktor waktu ini termasuk penundaan waktu yang melekat dalam diagnosis kegagalan; memperbaiki bagian, dan memperbaiki implementasi. Memperbaiki urutan adalah faktor penting. Misalnya mungkin perlu memulihkan tenaga listrik sebelum memperbaiki peralatan lain. Jumlah dan lokasi personel pemeliharaan memiliki pengaruh besar pada waktu pemulihan. Untuk sistem yang sangat kompleks, sumber daya memungkinkan, sangat berguna untuk memodelkan sistem dan mendukung kerentanan sistem, interdependensi, dan waktu rekonstitusi ketika mengalami ancaman yang berbahaya.
6. Menentukan Kerentanan: Proses penilaian kerentanan mempertimbangkan ancaman yang memiliki potensi secara individu atau kolektif untuk mempengaruhi satu atau lebih sistem kritikal. Berguna untuk membuat matriks (Gambar 3) untuk menghubungkan ancaman dengan sistem. Menentukan sistem mana yang akan dipengaruhi oleh ancaman yang jelas dalam beberapa kasus. Dalam kasus lain, mungkin perlu membandingkan tingkat dampak yang ditimbulkan oleh ancaman/kerawanan yang diidentifikasi dengan kekuatan sistem yang terpapar (misalnya kekuatan ledakan pada ruang produksi dibandingkan dengan kekuatan dinding). Setelah sistem kritikal ditentukan menjadi rentan, telusuri kegagalan kaskade dengan menentukan apakah sistem dependen lainnya dapat berhenti berfungsi sebagai akibat dari kegagalan sistem awal.

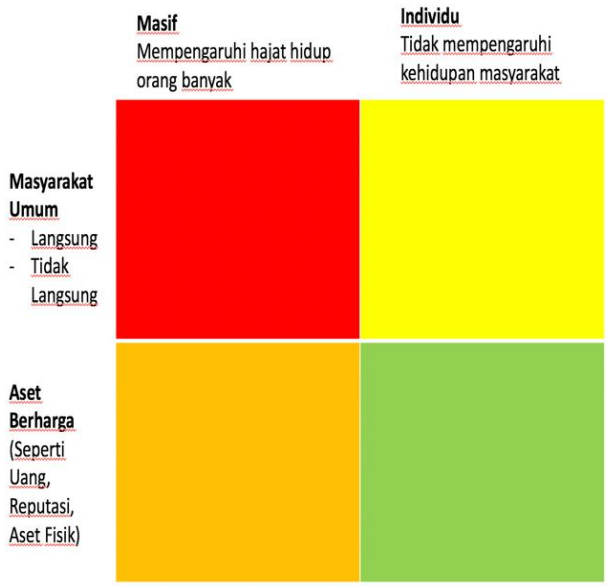
Kerentanna (Sistem Kritikal)	Komputer	Server, Router	Catu Daya	Fiber Optik	Aplikasi	Penyimpanan Data	Dan lainnya..
Serangan Siber							
Pemotongan Kabel							
Kebakaran							
Sabotase							
Gagalnya Layanan Elektrik							
Dan sebagainya ..							

Gambar 3. Contoh Matriks Kerentanan Sistem

Kerentanan titik tunggal menjadi perhatian khusus. Ini adalah tempat-tempat di dalam IKN yang mengumpulkan lebih dari satu sistem kritikal atau elemen sistem kritikal. Contohnya adalah ruangan yang berisi sistem utama dan cadangan, papan kontrol yang mengoperasikan fungsi normal dan darurat, lubang pembuangan yang mengakses beberapa kabel sistem (komunikasi, tenaga listrik) dan / atau pipa (air, bahan bakar, saluran tekanan). Gambar 4 memberikan contoh kerentanan umum.

Kerentanan yang diketahui dari insiden sebelumnya cukup instruksional. Insiden masa lalu memberikan pelajaran tidak hanya dari kerentanan sistem sudut pandang tetapi juga konsekuensi nyata. Data konsekuensi termasuk waktu henti sistem, biaya, fasilitas lain, dan organisasi yang terpengaruh dapat memberikan wawasan tentang peristiwa di masa depan yang serupa maupun tidak. Pertanyaan-pertanyaan berikut sangat membantu dalam menentukan kerentanan:

(1) Ancaman/kerawanan sistem seperti apa yang pernah Anda alami dan apa penyebabnya? (2) Sistem apa yang terpengaruh? (3) Apa jenis efek cascading yang diamati?



Gambar 4. Kerentanan Umum

7. Sistem Saling Ketergantungan : Peningkatan saling ketergantungan di antara sistem IKN dapat membuka peluang kegagalan sistem semakin besar. Sistem yang saling tergantung hanya dapat dilihat dari risiko yang dapat ditimbulkan dan berdampak ke sistem lainnya. Walaupun sulit untuk mengetahui kerentanan dari sistem dari hulu sampai hilir, lebih baik untuk mempertimbangkan efek atau dampak yang ditimbulkan terhadap proses bisnis sistem. Komunikasi di antara pemangku kepentingan yang saling tergantung dapat membantu meningkatkan ketahanan sistem yang lebih kompleks.

   a. Dependensi Hilir. Efek dari lemahnya sistem IKN satu sektor akan mengalir ke sistem sektor lain. Mulailah dengan mengembangkan daftar sistem IKN yang saling ketergantungan antar sektor. Pahami sejauh mana sistem IKN tersebut bergantung pada proses bisnis dan layanan sektor lain di IKN.

   b. Dependensi Hulu. Sistem IKN tergantung pada layanan dari sumber daya lainnya. Sekali lagi, penting untuk mengenali dan mendaftar ini. Identifikasi pemasok tunggal yang produk dan/atau layanannya tidak diduplikasi oleh pesaing. Pertimbangkan ancaman yang mungkin memengaruhi organisasi hulu dan coba perkirakan durasi waktu henti mereka dan dampaknya pada sektor IKN di bawah kondisi ancaman dan bahaya yang mungkin terjadi.

8. Personil dan Tanggung Jawab. Sistem fisik tidak ada gunanya tanpa adanya Sumber Daya Manusia (Personil). Mulailah dengan meninjau dan mengidentifikasi personil yang terlibat dalam sistem IKN tersebut. Tentukan personil utama yang diperlukan selama operasi normal. Apa tanggung jawab mereka? Kemudian pertimbangkan bagaimana persyaratan personil dapat berubah dalam kondisi bencana. Identifikasi fungsi tanpa operator cadangan. Identifikasi personil mana dan berapa banyak yang sudah dilatih untuk perbaikan dan prosedur penyelesaian jika terjadi kegagalan sistem normal dan darurat. Jika sektor IKN bergantung pada responden darurat di luar lokasi, seberapa jauh mereka dan berapa lama waktu respons mereka?

9. Daya tahan. Hal ini tergantung pada prosedur yang ada, suku cadang, dan kerusakan peralatan pemulihan untuk meminimalkan efek dan memulihkan operasi setelah insiden terjadi. Sangat penting untuk menentukan prosedur, protokol, dan individu yang bertanggung jawab jika terjadi kegagalan sistem. Faktor penting adalah keberadaan sistem cadangan di tempat dan waktu yang diperlukan untuk beralih ke sistem cadangan ini.

Perubahan Sistem yang Direncanakan. Sebagian besar fasilitas tidak statis. Perubahan peralatan dan konfigurasi adalah masalah rutin dan dapat sangat mengubah status kerentanan. Mempertimbangkan peningkatan atau perpindahan sistem yang direncanakan. Juga pertimbangkan perubahan besar pada pelengkap dan kemampuan personel. Sebagian besar fasilitas mengganti sistem sering berdasarkan persyaratan pemeliharaan atau peningkatan teknologi. Pertimbangan penting adalah frekuensi masa penggantian dan peningkatan sistem.

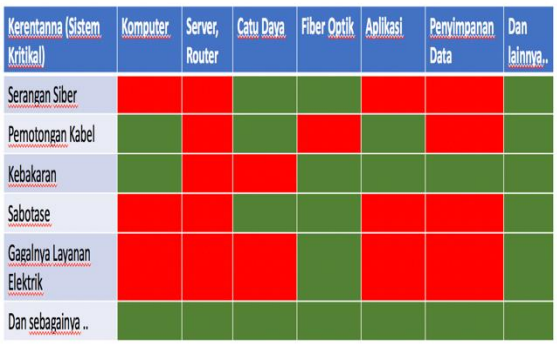
IV. HASIL DAN DISKUSI

Dari penilain kerentanan untuk menentukan kriteria IKN tersebut diatas, kemudian didapat hasil penilaian dan bagaimana cara mitigasinya sebagai berikut :

A. Hasil Penilaian Kerentanan IKN

Hasil penilaian memberikan informasi tentang kerentanan sistem IKN terhadap ancaman yang dapat ditimbulkan. Sangat membantu untuk memberikan ringkasan tertulis dari hasil penilaian untuk setiap sistem kritikal di sektor IKN. Ringkasan ini juga memberikan gambaran tentang kondisi sistem sebagai dasar untuk perbaikan di masa depan.

Matriks sistem/ancaman menjadi ringkasan hasil penilaian kerentanan. Contoh hipotetis untuk sektor telekomunikasi disediakan pada Gambar 5. Matriks ini berguna untuk mengevaluasi perilaku sistem ketika terkena berbagai ancaman. Matriks ini juga dapat digunakan sebagai daftar periksa saat pemutakhiran sistem selesai.



Gambar 5. Contoh Penilaian Kerentanan : Hasil Matrik Kerentanan Sistem

Contoh matriks menunjukkan bahwa banyak sistem kritikal tidak memiliki perlindungan yang seimbang; yaitu, kerentanan tidak seragam di semua kerawanan dan ancaman. Strategi investasi yang baik adalah memberikan perlindungan, suku cadang, dan / atau prosedur penyelesaian khusus untuk sistem-sistem dengan ancaman / kerawanan yang belum terselesaikan. Dalam contoh ini, ancaman paling serius di seluruh komponen sistem adalah kebakaran, bahan peledak, dan sabotase. Untuk fasilitas infrastruktur ini, jaringan komputer dan sistem telepon perlu paling diperhatikan.

Kerentanan umum termasuk akses tidak terbatas ke ruang teknik dan utilitas. Di banyak fasilitas, peralatan penting terkonsentrasi di satu lokasi. Beban api yang berlebihan membuat fasilitas rentan terhadap kecocokan. Sebagian besar fasilitas infrastruktur komersial belum mempertimbangkan kemungkinan serangan bom dalam desain atau operasi mereka. Bangunan dirancang menggunakan standar industri yang tidak mengkompensasi kegagalan bencana yang disebabkan oleh ledakan. Sebagian besar fasilitas tidak memantau kebocoran bahan berbahaya atau agen bio-kimia. Sebagian besar fasilitas tidak menyimpan bahan habis pakai untuk beroperasi di lingkungan pasca serangan.

Dalam banyak kasus, sistem kritis tidak memiliki kemampuan cadangan. Jika mereka melakukannya, sering kali sistem cadangan atau komponen dari sistem cadangan paling sering digabungkan dengan sistem primer. Dalam banyak kasus, sistem redundan dimasukkan ke dalam satu simpul kritis tunggal yang digunakan bersama oleh sistem primer. Contoh tipikal adalah panel distribusi listrik tunggal yang mengontrol aliran daya komersial, generator cadangan diesel, dan baterai pasokan daya tak terputus (UPS).

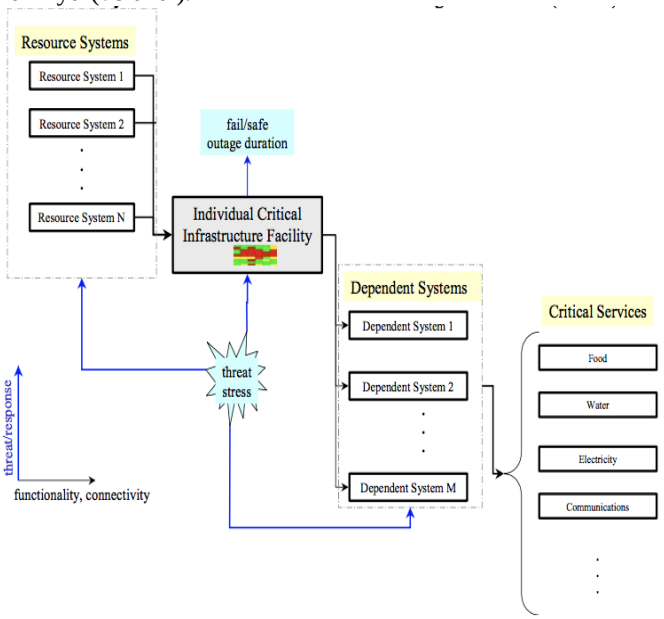
B. Mitigasi Kerentanan

Penilaian dapat mengidentifikasi opsi untuk mengurangi atau menghilangkan kerentanan yang diidentifikasi. Ada dua pendekatan dasar untuk ini: peningkatan peralatan dan peningkatan prosedural. Perbaikan prosedural lebih murah, dan efektif untuk sebagian besar masalah yang diidentifikasi. Sebagai salah satu contoh, hanya menghapus informasi tertentu dari situs web dapat mengurangi visibilitas teroris ke dalam operasi tersebut.

C. Penggunaan Hasil Penilaian Kerentanan pada Sektor IIKN

Metodologi yang diuraikan di atas dapat digunakan sebagai metodologi umum yang dapat diulang di semua sektor IKN. Banyak kesamaan dengan sistem pendukung di semua fasilitas sistem, seperti, sebagian besar fasilitas memiliki tenaga listrik, pemanas, ventilasi, pendingin udara, air, dan sistem komunikasi. Setiap fasilitas sektor IKN akan memiliki beberapa sistem unik yang akan memerlukan evaluasi khusus. Tetapi sistem pendukung fasilitas ada di mana-mana dan akan memiliki banyak kerentanan umum [4].

Metodologi tingkat fasilitas adalah fungsi dasar untuk penilaian kerentanan di masing-masing sektor IKN yang lebih penting dan lebih besar. Tujuan dari penilaian sektor IKN adalah untuk mengidentifikasi hambatan pada kemampuan untuk menyediakan layanan kritikal di sektor IKN. Mudah untuk mengidentifikasi layanan-layanan ini berdasarkan sektor. Maka penting untuk menentukan sistem yang diperlukan untuk layanan ini dan saling ketergantungan antar sektor [5]. Dengan mengumpulkan informasi tentang fasilitas sumber daya masing-masing fasilitas dan fasilitas dependen, dimungkinkan untuk mengembangkan diagram fungsional saling ketergantungan sektor. Skema untuk mengintegrasikan penilaian kerentanan di pemangku kepentingan ke dalam penilaian sektor digambarkan pada gambar 6. Secara konseptual, dalam skema ini interdependensi sistem mengalir dalam satu arah (horisontal dalam ilustrasi ini) dan ancaman terhadap sistem memengaruhi informasi dalam arah ortogonal lainnya (vertikal).



Gambar 6. Skema Penilaian Sektor IKN (Ref: Modeling Critical Infrastructure Requirements)

Setelah kerentanan masing-masing sistem diketahui, dimungkinkan untuk memahami efek gabungan pada kemampuan untuk menyediakan layanan kritis seperti yang ditunjukkan. Penting untuk melihat masalah baik dari pendekatan layanan ke sumber daya (kanan ke kiri pada skema) dan pendekatan sumber daya ke layanan (kiri ke kanan). Pendekatan pertama memberikan penghargaan untuk sistem tingkat atas yang diperlukan untuk fungsi sektor IKN. Yang kedua sangat membantu dalam mengidentifikasi pemasok tunggal sumber layanan dan komoditas yang diperlukan untuk infrastruktur operasional.

Dengan menggunakan skema ini, dimungkinkan untuk mengevaluasi titik lemah sistem yang menghambat proses bisnis dan layanan kritikal. Hal ini, tentu saja dapat bervariasi tergantung pada skenario ancaman. Skema ini menunjukkan diagram saluran tunggal yang mungkin berkaitan dengan satu sektor infrastruktur. Salah satu pendekatan adalah mengembangkan diagram tunggal untuk setiap sektor sebelum menggabungkannya ke dalam sektor IKN

V. SIMPULAN

Makalah ini menjelaskan metodologi penilaian kerentanan untuk sistem IKN dan secara singkat membahas integrasi hasil sistem IKN pada pemangku kepentingan ke dalam penilaian skala sektor IKN. Metodologi ini dirancang agar komprehensif dalam hal mengakomodasi ancaman fisik dan cyber terhadap rangkaian layanan dan proses bisnis kritikal di sektor IIKN. Sementara penekanannya adalah pada penilaian kerentanan, hasilnya memberikan banyak factor penting dari penilaian risiko secara keseluruhan. Metodologi ini berlaku untuk penilaian sendiri oleh penyedia layanan infrastruktur atau untuk digunakan oleh tim penilaian eksternal.

Metodologi ini menggabungkan matriks untuk mengidentifikasi kombinasi ancaman sistem yang paling kritikal untuk masing-masing IKN. Penerapan metodologi umum dibantu oleh keberadaan sistem pendukung serupa di sebagian besar sistem kritikal termasuk tenaga listrik, telekomunikasi, komputer, air, pemanas, ventilasi, dan sistem pendingin udara.

Metodologi ini dapat digunakan sebagai fungsi dasar untuk penilaian sektor IKN dalam menentukan hambatan dan kemampuan untuk menyediakan layanan kritis. Makalah ini menyediakan skema untuk mengintegrasikan penilaian kerentanan sistem ke dalam sektor IKN.

REFERENSI

[1] *Enisa. Methodologies for the Identificatio of Critical Information Infrastructure assets and service. 2014.*

[2] *Antonio García Zaballos, Inkyung Jeun, Best Practices for CriticalInformation Infrastructure Protection (CIIP) Experiences from Latin America and the Caribbean and Selected Countries, KISA – IDB, 2016*

[3] *Modeling is advised for highly complex systems. Commercial software is available for this purpose*. James Madison University is developing a Network Security Risk Assessment Model (NSRAM) tool that will be useful for this purpose. 2015

[4] Wolthusen, Stephen D., *Modeling Critical Infrastructure Requirements*, Proceedings of the 2004 IEEE Workshop on Information Assurance and Security, June 2004.

[5] *Rome NRome* NY. Protecting *People at Risk, Special Issue, Advanced Materials and Processes Technology Information Analysis Center Quarterly*, Volume 6, Number 4. 2015