Jurnal Kewarganegaraan
Vol. 6 No. 4 Desember 2022
P-ISSN: 1978-0184 E-ISSN: 2723-2328

Pembangunan Benteng Digital Pertahanan Indonesia

Unggul Satrio Yudhotomo[1] Selfira Salsabilla[2] Khaerudin[3] Timbul Siahaan[4]
Fakultas Teknologi Pertahanan, Universitas Pertahanan Republik Indonesia[1,3,4]
Fakultas Manajemen Pertahanan, Universitas Pertahanan Republik Indonesia[2]
Email: unggul_industryugm@yahoo.co.id[1]

Abstrak

Perkembangan teknologi yang sangat pesat memicu munculnya ancaman siber. Dampaknya tidak hanya pada bidang teknologi saja, namun juga mengancam berbagai bidang kehidupan seperti Pertahanan keamanan negara, ekonomi, ideologi, politik, sosial, dan budaya. Sehingga diperlukan adanya inovasi teknologi berupa cyber security yang handal dan terintegrasi dalam perlindungan data dan keamanan informasi semacam Benteng Digital yang mampu menangkal ancaman. Namun, cyber security di Indonesia dinilai masih belum cukup tangguh. Untuk memperkuat cyber security di Indonesia, sebaiknya dilakukan penguatan lima fondasi dasarnya, meliputi: kepastian hukum, prosedur tindakan teknis, struktur organisasi; capacity building, dan pendidikan bagi pengguna perangkat siber. Salah satu bentuk inovasi cyber security adalah sistem control access dan firewall.
Kata Kunci: Inovasi Teknologi, Perlindungan Data, Keamanan Informasi

Abstract

Rapid technological developments trigger the emergence of cyber threats. The impact is not only in the field of technology, but also threatens various fields of life such as national security, economic, ideological, political, social and cultural defense. So that there is a need for technological innovation in the form of cyber security that is reliable and integrated in data protection and information security such as a Digital Fortress that is able to ward off threats. However, cyber security in Indonesia is considered not strong enough. To strengthen cyber security in Indonesia, it is advisable to strengthen the five basic foundations, including: legal certainty, technical action procedures, organizational structure; capacity building, and education for cyber device users. One form of cyber security innovation is access control systems and firewalls.
Keywords: *Technological Innovation, Data Protection, Information Security*

PENDAHULUAN

Dalam masa *internet of things* yang mana ancaman peretasan sangat massif dengan berbagai macam tujuan. Hal ini dikenali sebagai ancaman nasional terlebih negara dapat saja lumpuh dengan menguasai system IT atau information teknologi di suatu negara maka ini dapat mengkontrol dalam keinginan peretas tersebut. Potensi era industri 4.0 memperluas spektrum ancaman yang awalnya berada di ranah darat, laut, udara menuju dimensi ruang angkasa dan siber. Dalam perkembangan teknologi informasi dan komunikasi tersebut, banyak pihak baik individu atau kelompok bahkan tidak menutup kemungkinan pada level negara, memiliki tujuan tidak baik untuk mencapai keuntungan pribadi atau bahkan mencapai tujuan dalam kepentingan politik suatu negara. Tujuan-tujuan tersebut dicapai dengan melakukan serangkaian aktivitas ilegal dalam ruang siber.

Secara konsep, perlawanan dalam ruang siber inilah yang kita kenal dengan Perang Siber/Cyber Warfare, yang berarti Perang yang dilakukan dengan mengerahkan kekuatan, segala kemampuan dan teknologi dalam kecanggihan sistem komputer (Kementerian Pertahanan Republik Indonesia, 2020). Kemudian dampak terburuk bila tujuan dari pihak tidak bertanggung jawab itu tercapai, dapat merebak lebih luas dengan terwujudnya bentuk perang modern lainnya yaitu Network Centric Warfare dan Perang Proxy. Perkembangan ilmu

pengetahuan mengenai pertahanan siber di tingkat internasional sudah maju. Pemerintah dapat melakukan banyak aktivitas pemerintahan hanya melalui internet dan komputer, seperti melaksanakan pertemuan diplomatik tanpa perlu hadir secara fisik, melakukan pengarsipan dokumen-dokumen negara secara digital, membangun data dan pusat informasi, dan masih banyak lagi. Namun pada prakteknya di Indonesia masih terdapat GAP dalam memperkuat perlindungan data dan informasi, sehingga seringkali kita mendapati adanya isu cyber attack, kebocoran data yang sangat berpotensi dimanfaatkan oleh pihak tertentu yangtidak bertanggung jawab untuk tujuan melakukan tindak kejahatan (cyber crime). pertahanan dari ancaman siber yang dapat diretas, dirusak dan mengganggu seluruh sistem Pertahanan RI.

Gambar 1. Diagram Analisis SWOT

Dalam diagram analisis SWOT diatas dapat di peroleh hasil observasi pada lemahnya Kondisi Benteng Digital saat ini. Kemampuan peralatan Badan Operasional Keamanan Jaringan alias Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTI) tidak memadai untuk memantau serangan. Contohnya Kementerian, Lembaga, dan Perbankan selama ini masih sering kebobolan. Dalam waktu dekat Indonesia harus memiliki sistem keamanan yang dapat dikategorikan canggih dan memiliki kemampuan melindungi dari serangan cyber atau potensinya. Sangat penting sekali pemerintah segera memperkuat lagi Badan Cyber Nasional (BCN) yang dapat menjadi jendral sebagai pengamanan data dan informasi nasional dan menjadi koordinator untuk mengawal data negara dan menngindari ancaman besar atas kekacauan informasi dan data negara.

Potensi serangan atau Threat di Internet meningkat dengan tajam seiring dengan pesatnya kecanggihan teknologi. Bukan hanya sektor bisnis, sektor kementerian dan lembaga, tapi sektor publik juga menjadi serangan. Hacktivism sangat expansif sebagai akibat terhadap isu nasional ataupun kejadian nasional dan juga usaha untuk menguji system pertahanan terhadap ancaman digital kita. Contoh serangan lainnya nyata terhadap meningkatnya serangan, termasuk sektor publik. Sistem keamanan harus terus dilakukan pembaruan.

METODE PENELITIAN

Penelitian ini menggunakan metode analisis deskriptif dengan pendekatan kualitatif. Teknik pengumpulan data dalam artikel ini menggunakan sumber data sekunder yang diambil dari buku, surat kabar online, jurnal, artikel, dan dokumen lainnya yang relevan dengan topik artikel. Penelitian dimaksudkan untuk menganalisis data dengan menggunakan teknik reduksi data sebagai dasar dalam mengeksplorasi bagaimana membangun benteng digital untuk perlindungan data dan informasi penting di Kementerian/Lembaga pemerintah dalam rangka memperkuat pertahanan siber nasional. Dimana pembangunan benteng digital ini sangatlah diperlukan karena pembelian ALPALHANKAM terbaru disertai teknologi canggih yang dapat di remote. Kecangihan inilah yang justru menjadikan ancaman bagi negara karena bisa saja alat alat canggih yang kita miliki dapat diretas.

HASIL PENELITIAN DAN PEMBAHASAN

Dengan dijabarkannya permasalahan diatas maka dapat ditarik hasil Observasi adalah kurang cepatnya pembangunan Benteng Pertahanan Digital. Hal ini terjadi disebabkan adanya kekurangan dari sumber daya Manusia yang sadar akan pentingnya Benteng Digital bagi ekamanan sebuah negara. Terutama di era teknologi canggih yang berkembang dengan cepat dan bahkan dengan akses *IoT* atau *Internet Of Thing* yang semua akan dapat diakses secara global. Dengan mengetahui kelemahan ini bertujuan untuk membenahi agar dapat menjadi Projek Prioritas bagi keamanan Negara. Hasil Kajian dan penelitian dapat menjadi dasar pemerintah mengatur ulang Prioritas pembangunan keamanan digital di Indonesia yang masih sangat rapuh . Dengan paparan semua komponen dan factor dapat dijadikan *overview* dan bermanfaat dalam pengembangan pengembangan yang komprehensif dalam pembangunan kekuatan tangkal peretasan dan hacking oleh penjahat yang bersifat merugikan system di Indoensia. Sistem yang terdapat suatau negara adalah tanggung jawab pemerintah untuk menjamin keamanannya. Karena sangat berkait dengan stabilitas keamanan bahkan sampai sector ekonomi.

Pemetaan Ancaman Siber

Ancaman siber adalah tindakan yang mungkin muncul namun berpotensi menyebabkan masalah serius terhadap jaringan atau sistem komputer dan semua orang bisa terkena dampaknya (CIPS, 2021). Lemahnya kekuatan benteng digital di lingkungan kementerian/ Lembaga pemerintah telah dibuktikan dengan serangkaian kejadian data kementerian dan data negara yang diretas. Contohnya sepanjang tahun 2021 saja, berbagai situs resmi milik pemerintah seperti BPJS Kesehatan (bpjs-kesehatan.go.id), Sekretariat Kabinet RI (setkab.go.id), aplikasi *Electronic Health Alert* (e-HAC) milik Kementerian Kesehatan, hingga Pusat Malware Nasional (Pusmanas) milik Badan Siber dan Sandi Negara (pusmanas.bssn.go.id) dan database milik Polri diretas dalam bentuk pembocoran data dan *deface* (pengubahan tampilan halaman pada target situs) (Kompas.com, 2021).

Salah satu bentuk tindakan preventif untuk membentuk daya tangkal yang kuat dan berkelanjutan dalam dimensi teknologi siber adalah pembangunan pertahanan atau benteng digital Indonesia, terlebih pada Kementerian/Lembaga pemerintah. Sebagaimana dicantum dalam Kebijakan Umum Pertahanan Negara 2020-2024 pada kebijakan pembangunan postur pertahanan nirmiliter, pembangunan kemampuan dilaksanakan melalui peningkatan kualitas sumber daya manusia, serta sarana dan prasarana kementerian, lembaga, dan pemerintah daerah dengan memanfaatkan perkembangan teknologi. Sebagai contoh dalam menghadapi cyber war di antaranya upaya serius pemerintah Amerika Serikat dalam mengembangkan The *National Cyber Security Division* (NCSD) atau satu divisi khusus yang bertugas menangani keamanan *cyber* secara nasional yang didukung oleh sektor swasta dan masyarakat yang memiliki tugas untuk membangun dan memelihara nasional yang efektif sistem keamanan cyber atau dunia maya.

Global cyber-security dibangun diatas lima bidang kerja: Kepastian hukum (undang-undang *cyber crime*); Teknis dan tindakan prosedural (pengguna akhir dan bisnis (pendekatan langsung, penyedia layanan, dan perusahaan perangkat lunak); Struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih); *Capacity building* dan Pendidikan pengguna (kampanye publik dan komunikasi terbuka dari ancaman *cyber crime* terbaru); Kerjasama Internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman siber).

Kontrol Akses dan Teknologi *Firewall*

Fitur paling penting dari kontrol akses adalah untuk memverifikasi identitas pengguna yang mengakses sumber daya komputer. Dibutuhkan audit, verifikasi otorisasi, kata sandi, kunci, dan metode otentikasi lainnya untuk melindungi pengguna keamanan informasi dan komputer. Sederhananya, ide inti dari kontrol akses adalah bahwa informasi hanya terbuka pengguna yang benar-benar membutuhkannya, dan bahwa pengguna yang masuk secara ilegal dicegah. Kontrol akses merupakan sarana penting untuk melindungi keamanan jaringan komputer. Karena hal ini memiliki efek yang baik pada blokade hacker dengan semua akses kontrol yang tidak sembarangan orang dapat mengakses mengurangi resiko terjangkitnya sistem keamanan jaringan oleh virus nakal yang dapat meretas dan bersifat *spy*.

Gap Kondisi saat ini dan Kondisi yang diharapkan RUU Keamanan Siber menunjuk BSSN untuk mengkoordinasikan upaya pengembangan strategi keamanan siber dengan berkolaborasi dengan lembaga pemerintahan lainnya, seperti Kementerian Komunikasi dan Informatika (Kominfo), Badan Intelijen Nasional (BIN), Kepolisian Republik Indonesia, dan Tentara Nasional Indonesia (TNI). Akan tetapi, RUU tersebut tidak merinci peran antar lembaga-lembaga tersebut, dan juga tidak menjabarkan tanggung jawab BSSN dan lembaga pemerintahan lainnya dalam melindungi keamanan siber. Pasal 38 menyebutkan bahwa BSSN dapat menyaring konten dan aplikasi elektronik yang mengandung konten berbahaya guna melindungi keamanan masyarakat ketika menggunakan aplikasi elektronik. Akan tetapi, tugas menyaring konten dan aplikasi saat ini dilakukan di bawah wewenang Kominfo. Sayangnya, pasal 38 tersebut tidak mengatur koordinasi antara BSSN dan Kominfo untuk menyaring konten, dan tidak ada kriteria yang rinci terkait apa yang dianggap konten berbahaya.

Selain tidak adanya penjabaran wewenang yang jelas antara BSSN dan lembaga pemerintah terkait lainnya, asosiasi pengusaha juga mengkritik Pasal 4 dan 8 karena membatasi keterlibatan sektor swasta dan asosiasinya dalam masalah keamanan siber (Wibowo, 2019). Pasal 4 dari RUU tersebut menyatakan bahwa keamanan siber akan dilaksanakan oleh lembaga pemerintah, pemerintah pusat, pemerintah daerah, dan masyarakat. Menurut Pasal 8, masyarakat bisa terlibat dalam pelaksanaan keamanan siber ketika melindungi sistem elektronik internal perusahaan mereka atau ketika menyediakan layanan untuk keamanan siber. Namun, penggunaan kata "masyarakat" dinilai sangat luas dan mungkin tidak diinterpretasikan secara khusus untuk melibatkan semua pemangku kepentingan di sektor swasta.

Pada pasal 66 RUU Keamanan Siber mewajibkan para pengusaha untuk memenuhi persyaratan kandungan lokal, yaitu 50% Tingkat Komponen Dalam Negeri (TKDN). Mengingat kebanyakan pengusaha menggunakan perangkat keras dan lunak dari luar negeri untuk produk dan jasa mereka, maka persyaratan 50% TKDN akan berdampak pada pengembangan produk dan jasa keamanan siber di Indonesia. Semua pasal yang disebutkan seakan berlawanan dengan tujuan untuk meningkatkan persaingan dan inovasi siber melalui penggunaan siber yang bebas, terbuka, dan bertanggung jawab seperti yang tercantum pada Pasal 3 (b) RUU Keamanan Siber. Tujuan tersebut hanya bisa dicapai dalam sebuah dialog yang sarat makna dengan pemangku kepentingan yang relevan dari sektor pengusaha, akademisi, dan masyarakat.

UU 11/2008 dan PP 82/2012 sebagai Dasar Keamanan Siber dan Pertahanan Siber Semesta

UU No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem Dan Transaksi Elektronik merupakan pondasi membangun Keamanan Siber dan Pertahanan Siber nasional

secara organik. Secara organik maksudnya keamanan dan pertahanan nasional dibangun oleh Penyelenggara Sistem Elektronik secara semesta dan berkesinambungan. Pasal 15 UU ITE mengatur bahwa Penyelenggara Sistem Elektronik harus menyelenggarakan sistem elektroniknya secara aman, andal, dan bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya. Artinya seluruh Penyelenggara Sistem Elektronik, terlepas apakah sistem itu digunakan untuk kepentingan pemerintahan, komersial, atau pribadi harus menyelenggarakan sistemnya secara andal, aman dan bertanggung jawab.

PP 82/2012 memberikan pedoman bagaimana Penyelenggara Sistem Elektronik menyelenggarakan sistemnya secara andal, aman, dan bertanggung jawab sebagaimana diamanatkan oleh UU ITE. Kemudian PP 82/2012 mengatur bahwa Sistem Elektronik memiliki lima komponen, yaitu: Perangkat keras, Perangkat lunak, Tenaga ahli, Tata kelola dan Pengamanan. Menurut UU No. 3 Tahun 2002 tentang Pertahanan Negara, pertahanan negara adalah segala usaha untuk mempertahankan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan keselamatan segenap bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara. Sistem pertahanan negara Indonesia bersifat sistem pertahanan semesta, yaitu melibatkan seluruh warga negara, wilayah, dan sumber daya nasional lainnya, serta dipersiapkan secara dini oleh pemerintah dan diselenggarakan secara total, terpadu, terarah, dan berlanjut untuk menegakkan kedaulatan negara, keutuhan wilayah, dan keselamatan segenap bangsa dari segala ancaman.

Koordinasi Keamanan Siber dan Pertahanan Siber

Meskipun UU 11/2008 dan PP 82/2012 telah meletakan dasar pengaturan untuk membangun sistem Keamanan Siber dan Pertahanan Siber yang bersifat semesta, diperlukan kontrol, koordinasi, dan pengawasan secara strategis dan efektif. Kementerian Komunikasi dan Informatika memiliki tugas dan fungsi di bidang Telekomunikasi, Informatika, Penyiaran, dan Pos. Keempat bidang ini sangat berperan dalam membangun dan mengembangkan Keamanan Siber dan Pertahanan Siber secara holistik. Budaya Keamanan Informasi di masyarakat perlu ditumbuhkan, Dalam keadaan perang, seluruh sumber daya digunakan untuk mempertahankan Sistem Elektronik khususnya yang strategis dan meredam serangan siber dan menyerang untuk melumpuhkan serangan. Dalam kondisi perang, Tentara Nasional harus lebih berperan aktif.

Perlunya Strategi Nasional Keamanan Siber dan Pertahanan Siber

Adanya serangan siber (cyber attack) yang tidak dilangsungkan atas nama negara tertentu. Oleh karena itu, Kementerian Kominfo dan Kementerian Pertahanan serta Kementerian Koordinator Polhukam harus bekerja sama secara intensif. Instansi-instansi ini perlu bekerja sama dalam membuat Strategi Nasional Keamanan Siber dan Pertahanan Siber. Strategi dimaksud perlu dibentuk dalam suatu Rencana Besar (master plan) yang berisi, antara lain:

1. Penentuan dan evaluasi ancaman (threat) dan kelemahan (vulnerabilities) Sistem Elektronik Infrastruktur Strategis di Indonesia
2. Pengelolaan sumber daya (khususnya manusia, teknologi, serta Penelitian dan Pengembangan R&D) dan untuk penguatan Keamanan Siber dan Pertahanan Siber
3. Pembangunan dan pengembangan sistem Keamanan Siber dan Pertahanan Siber semesta
4. Penentuan prioritas penguatan Sistem Elektronik Infrastruktur Strategis.

Kerangka Pemikiran Penyelesaian

Manajemen Teknologi Informasi Ada 4 (empat) pondasi utama yang mendukung perkembangan teknologi informasi yaitu: perkembangan perangkat lunak (*software*) seperti

sistem dan aplikasi dan perkembangan alat keras (*hardware*) perkembangan sarana dan prasarana teknologi informasi, manajemen isi (*content management*), *telecommunication and networking*, perkembangan internet serta perdagangan online atau melalui internet. Sementara untuk pengorganisasian terkait dengan pengunaan sistem teknologi informasi setidaknya ada empat hal utama yang harus diperhatikan yaitu: pertama, sistem informasi (*information systems*) dan kedua, kompetisi organisasi (*organizational competition*); ketiga, *information systems* (sistem informasi) dan *organizational decision making* (sistem informasi dan pengambilan keputusan dalam organisasi); keempat, pengorganisasian penggunaan sistem informasi (*organizational use of information systems*). Pada dasarnya sistem informasi itu terintegrasi, teknologi informasi dibangun berbasis sistem yang dirancang untuk dapat mendukung kerja, manajemen dan pengambilan keputusan dalam organisasi.

Solusi untuk Menjawab Permasalahan

Penjabaran Permasalahan yang sangat penting diatas menjadi sangat urgent sekali untuk membangun siatu system keamanan terpadu antara Pemerintah, militer dan pihak ahli atau ekosistem Teknologi informasi di Indonesia. ruang lingkup cyber-security dimulai dari install, harden atau keamanan terkait dengan perangkat keras yang digunakan dalam mengoperasikan internet, monitor, yang menyebabkan terjadinya insiden atau kejadian dan insiden itu dapat pula berasal dari serangan atau *cyber attact* yang membutuhkan penangganan terhadap insiden tersebut dengan melakukan uji forensik sebagai pembuktian dalam penegakan hukum terhadap terjadinya *cyber crime*. *Cyber-security* lebih lanjut dimaknai sebagai semua mekanisme yang dilakukan untuk melindungi dan meminimalkan gangguan kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan *(availability*) informasi. Mekanisme ini harus bisa melindungi informasi baik dari physical attack maupun *cyber attack*. *Cyber-security* merupakan upaya untuk melindungi informasi dari adanya *cyber attack,* adapun elemen pokok *cyber-security* adalah:

1. Dokumen *security policy* merupakan dokumen standar yang dijadikan acuan dalam menjalankan semua proses terkait keamanan informasi.
2. *Information infrastructure* merupakan media yang berperan dalam kelangsungan operasi informasi meliputi *hardware* dan *software.* Contohnya adalah *router, switch*, server, sistem operasi, *database*, dan *website*.
3. *Perimeter Defense* merupakan media yang berperan sebagai komponen pertahanan pada infrastruktur informasi misalnya IDS, IPS, dan *firewall.*
4. *Network Monitoring System* merupakan media yang berperan untuk memonitor kelayakan, utilisasi, dan *performance* infrastruktur informasi.
5. *System Information and Event Management* merupakan media yang berperan dalam memonitor berbagai kejadian di jaringan termasuk kejadian terkait pada insiden keamanan.
6. *Network Security Assessment* merupakan elemen *cyber-security* yang berperan sebagai mekanisme kontrol dan memberikan measurement level keamanan informasi. *Human resource dan security awareness* berkaitan dengan sumber daya manusia dan *awareness-nya* pada keamanan informasi. Selain *cyber-security* kelangsungan operasi informasi juga bergantung pada physical security yang tentunya berkaitan dengan semua elemen fisikal misalnya bangunan data center , *disaster recovery system*, dan media transmisi.

Capacity Building

Dengan adanya komando khusus satuan cyber pengelolaan terhadap manajemen risiko dunia maya melalui upaya seperti peningkatan pelatihan, informasi tentang keamanan dan kerahasiaan serta pembangunan jaringan yang aman dan tangguh hingga membentuk industri pertahanan cyber yang tangguh antara lain dengan membuat program-program pertahanan dan

perlindungan cyber yang dapat digunakan untuk melindungi berbagai system. pelayanan publik dan pemerintahan serta militer dari serangan di dunia maya tidak hanya berupa Tim Kerja Pusat Operasi Dunia Maya (Cyber Defence Operation Centre) hal ini tertuang sebagaimana dibentuk oleh Kemenhan. Pengorganisasian terkait dengan cyber security tersebut hendaknya selaras dengan pengorganisasian pengunaan sistem teknologi informasi dengan memperhatikan empat hal utama yaitu: pertama, sistem informasi (information systems) dan kedua, kompetisi organisasi (organizational competition); ketiga, information systems (sistem informasi) dan organizational decision making (sistem informasi dan pengambilan keputusan dalam organisasi); keempat, pengorganisasian penggunaan sistem informasi (organizational use of information systems). Pengembangan cyber security itu terintegrasi, teknologi informasi dibangun berbasis sistem yang dirancang untuk dapat mendukung kerja, manajemen dimana cyber-security tersebut dibangun. Selain itu Kedua, pembangunan sistem informasi. Ketiga, sumber daya eksternal sistem informasi. Keempat, manajemen sumber daya informasi.

Gambar 2. Faktor Pembangunan Benteng Digital

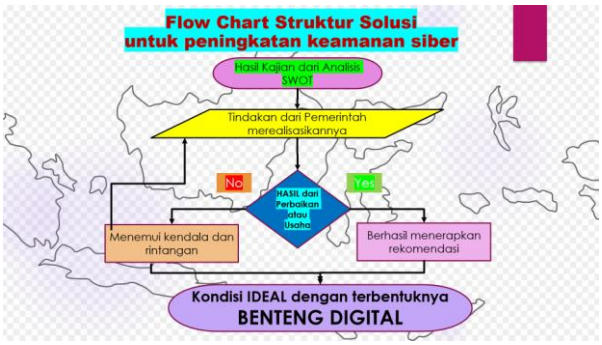
Dengan hasil Observasi terkait keamanan negara dalam kaitannya dengan Benteng Digital ini direkomendasikan "Masa Depan keamanan Siber Indonesia" dengan menggali berdasarkan lima dimensi cakupan Kapasitas Keamanan Siber yang terdiri dari komponen-komponen sebagai berikut:

1. Kebijakan dan Strategi keamanan Siber. Dokumen strategi nasional keamanan siber; Respon terhadap insiden; Perlindungan terhadap kritis nasional; Manajemen krisis; Perhatian terhadap keamanan siber; dan Redudansi sistem elektronik.
2. Budaya dan Masyarakat Siber. Pola pikir keamanan siber; Kesadaran keamanan siber; Keyakinan dan kepercayaan pengguna di internet; dan Privasi daring.
3. Pendidikan, pelatihan dan keterampilan keamanan siber. Ketersediaan pendidikan dan pelatihan nasional bidang keamanan siber; Pengembangan pendidikan nasional bidang keamanan siber; Prakarsa pendidikan dan pelatihan keamanan siber di dalam sektor publik dan swasta; dan Tata kelola organisasi, pengetahuan, dan standar.
4. Kerangka hukum dan peraturan keamanan siber. Kerangka kerja hukum keamanan siber; Fungsi dan kewenangan penyelidikan, penyidikan, dan penuntutan tindak pidana siber; dan Alur laporan pertanggung jawaban terhadap kerentanan dan kebocoran sistem elektronik.
5. Standar, organisasi, dan teknologi keamanan siber. Kepatuhan terhadap standar; Ketahanan infrastruktur nasional; dan Pasar keamanan siber.

Bila disimpulkan dengan menggunakan diagram Archetypes: Growth & Underinvestment akan tergambar sebagai berikut:

Gambar 3. ***Archetypes: Growth & Underinvestment***

Penjelasan: Dorongan pemerintah untuk regulasi dan paying hukum untuk keamanan siber Akan mendorong habitat kemanan siber dan juga menjamin perkembangan software builder dan juga trend ancaman menjadi terpetakan. Berdampak juga pada proses selanjutnya/pengolahan Sumber daya yang ada menjadi satu tameng system keamanan terhadap ancaman. Dengan memiliki kualitas ekosistem baik tentunya akan menciptakan Solusi dan inovasi dalam menegmbangkan system keamanan yang terpadu terutama oada sector militer dan pertahana keamanan yang kuat, sebagaimana tantangan dari tren-tren ancaman yang terus berkembang dalam masa era digital dan juga perkembangan yang derasnya arus ragam informasi yang terdistribusi secara bebas dan juga akses yang sangat luas. teknologi global meningkat dan dengan cepat menggilas siapa saja yang tidak mau mengikuti perkembangan zaman, dalam konteks era Teknologi informasi yang akan bermuatra ke dalam suatu jagat maya yang dapat mengkontrol jagat nyata, dan bisa digunakan untuk maksud maksud yang tidak baik. Struktur untuk Solusi dalam diagram berikut:



Gambar 4. Solusi Peningkatan Keamanan Siber

Pada Gambar diatas ini kita melakukan apa dari rekomendasi hasil dari analisis SWOT dan juga akan di kroscek pada implementasi dengan melakukan pembenahan namun pasti ada rintangan, dalam keadaan ideal akan bergeser kearah yang diinginkan namun jika ada kendala dan rintangan akan balik ke kondisi dimana pemerintah harius lebih serius lagi melakukan pembenahan. Adapun beberapa hal yang bisa dilakukan untuk penguatan ekosistem dari personil dan Teknologi Informasi yang menunjang pembangunan BENTENG DIGITAL dan Infrastruktur dalam rangka menciptakan kekuatan pertahanan serangan siber atau digital.

Keterkaitan *Cyber Security* (Keamanan Siber) dan *Cyber Defense* (Pertahanan Siber)

Keamanan Siber dan Pertahanan Siber memiliki setidaknya satu keterkaitan erat, yaitu bahwa keduanya diterapkan untuk menjaga dan mempertahankan kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) informasi elektronik atau Sistem Elektronik. Keamanan Siber dapat berupa salah satu bentuk dari Pertahanan Siber. Di lain pihak, Pertahanan Siber dapat berupa pertahanan aktif maupun pertahanan pasif. Pertahanan pasif yang dimaksud dapat tercakup dalam ruang lingkup Keamanan Siber.

Keamanan Siber maupun Pertahanan Siber dapat diselenggarakan oleh individu, kolektif maupun negara. Masing-masing ruang lingkupnya dapat berbeda. Keamanan Siber dan Pertahanan Siber yang diselenggarakan oleh negara dimaksudkan untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi penting bagi negara, keamanan nasional, maupun menjaga Sistem Elektronik yang strategis atau kritis bagi kelangsungan pelayanan publik atau kelangsungan negara. Pihak swasta maupun pribadi memiliki kepentingan untuk membangun keamanan dan mempertahankan informasi dan sistem elektroniknya untuk menjaga informasi dan sistem elektroniknya sesuai dengan kepentingannya masing-masing.

KESIMPULAN

Manajemen risiko untuk dunia cyber guna melindungi infrastruktur telekomunikasi dan cyber dari situasi kritis yang dikenal dengan the National Cyber space Response System. Terkait dengan pengembangan strategi nasional dalam membangun cyber- security di Indonesia ke depan dilakukan dengan memenuhi empat pondasi yang mendukung perkembangan teknologi informasi termasuk didalamnya pengembangan cyber-security yaitu: perkembangan perangkat lunak (software) seperti sistem dan aplikasi dan perkembangan alat keras (hardware) perkembangan sarana dan prasarana teknologi informasi, manajemen isi (content management), telekomunikasi dan networking, perkembangan internet serta perdagangan online atau melalui internet. Selain memenuhi keempat pondasi utama pengembangan cyber-security langkah lainnya yang mutlak dilakukan adalah pengorganisasian terkait dengan pengunaan sistem teknologi informasi dengan memperhatikan empat hal utama yaitu: pertama, sistem informasi (information systems) dan kedua, kompetisi organisasi (organizational competition); ketiga, organizational decision making (pengambilan keputusan dalam organisasi); keempat, pengorganisasian penggunaan system informasi (organizational use of information systems).

Secara singkat, cyber security ke depan hendaknya dibangun atas lima bidang dasar yaitu adanya kepastian hukum (undang-undang cyber crime); teknis dan tindakan prosedural pengguna akhir dan bisnis (pendekatan langsung penyedia layanan dan perusahaan perangkat lunak); Struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih); Capacity building dan pendidikan pengguna (kampanye publik dan komunikasi terbuka dari ancaman cyber crime terbaru); Kerjasama Internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman cyber), sehingga berita rahasia negara dapat terjamin keamanannya. Di Indonesia, perlu adanya peningkatan dan pengembangan software firewall dan perlu adanya peningkatan kemampuan atau adanya kompetensi operator program firewall Indonesia. Seiring dengan pesatnya penetrasi jaringan global dan kemajuan mobile Internet di Indonesia, semakin menambah kerentanan keamanan informasi sebuah organisasi dari ancaman siber (cyber threat). Serangan siber menjadi tantangan tersendiri untuk pemangku kebijakan pada era informasi.

Terdapat 5 (lima) rekomendasi yang telah dirumuskan pada kegiatan penyusunan kajian Pengembangan Keamanan Siber Nasional antara lain: Memperkuat kelembagaan keamanan siber dalam wujud pusat keamanan siber nasional sebagai rujukan utama dalam penanganan ancaman keamanan siber; Meningkatkan kerjasama dan peran aktif dalam peningkatan keamanan siber melalui kerjasama bilateral, multilateral, dan public-private partnership, termasuk kerjasama di tingkat nasional untuk mengembangkan national interconnected global intranet; Meningkatkan penguasaan teknologi keamanan siber untuk mengantisipasi berbagai ancaman serangan siber yang berasal dari dalam maupun luar negeri; Meningkatkan edukasi dan pengembangan kapasitas sumber daya manusia keamanan siber dan sarana prasarana penunjang lainnya seperti standar kompetensi kerja nasional serta lembaga pelatihan dan sertifikasi kompetensi keamanan siber; dan Menyusun dan menerapkan strategi pengembangan Keamanan Siber Nasional secara berkelanjutan untuk melindungi infrastruktur kritis nasional dan kedaulatan Negara.

DAFTAR PUSTAKA

http://ilmukomputer.org/wp-content/uploads/2015/05/apa-itu-iotinternet-of-things.pdf
http:/www.academia.edu/12418429/PengertianInternetOfThings
https://idsirtii.or.id/bssn.html bidang Persandian di Lemsaneg bidang keamanan informasi, pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet.

https://www.kominfo.go.id/content/detail/1805/id-sirtii-jadi-punggawa-pengawas-internet-asia-pasifik/0/sorotan_media
https://www.kompas.tv/article/200111/dua-remaja-pembobol-situs-setkab-punya-peran-berbeda-dan-berpengalaman-bobol-650-website
Https://Www.Researchgate.Net/Publication/282855443_Internet_Of_Things_Sejarah_Teknologi_Dan_Penerapannya_Review
Nathalie Chaplan, Cyber War: the Challenge to National Security, Global Security Studies,Winter 2013, Volume 4, Issue 1, University of North Carolina Wilmington
Pemerintah Indoensia, Peraturan Menteri Komunikasi dan Informatika No. 29/Per/M.Kominfo/12/2010 tentang perubahan kedua Peraturan Menteri Komunikasi dan Informatika No.26/PER/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet
Pemerintah Indonesia Peraturan Nomor 24 Tahun 2008 Tentang Penyelenggaraan Sistem Komunikasi Dan Elektronika Pertahanan Negara.
Pemerintah Indonesia, 2017. Perpres Nomor 53 Tahun 2017 Tentang Badan Siber dan Sandi Negara. bidang keamanan siber Jakarta
Pemerintah Indonesia, 2021. Perpres Nomor 28 Tahun 2021 Tentang Badan Siber dan Sandi Negara, keamanan, pelindungan, dan kedaulatan siber nasional. Jakarta
Pemerintah Indonesia. 2002. Undang-Undang Republik Indonesia Nomor 3 Tahun 2002 tentang Pertahanan Negara.Dalam pengelolaan sistem pertahanan negara. Jakarta.