IMPLEMENTASI MANAJEMEN RISIKO PERTAHANAN SIBER KEMENTERIAN PERTAHANAN UNTUK MENDUKUNG PERTAHANAN NEGARA

THE MINISTRY OF DEFENCE RISK MANAGEMENT IMPLEMENTATION TO SUPPORT THE COUNTRY'S DEFENSE

Doly Andhika Putra[1], Herlina J.R. Saragih[2], G. Royke Deksino[3]

UNIVERSITAS PERTAHANAN
(doly17andhika@gmail.com, herlinsara897@gmail.com,
georgeroykedeksino@gmail.com)

Abstrak – Arus globalisasi yang terjadi di seluruh dunia saat ini telah membawa dunia pada era perkembangan teknologi informasi dan komunikasi sehingga menciptakan era yang serba digital atau *digital world*. Perkembangan jaringan internet merupakan bagian dari budaya manusia yang terus berevolusi mencari kesempurnaan tanpa batas dalam mencapai kemudahan berkomunikasi. Dari perspektif pertahanan siber *(cyber defense)* pemanfaatan internet juga dimungkinkan untuk tujuan negatif atau *destruktif* oleh pihak-pihak yang mempunyai kemampuan. Fasilitas yang tersedia di ruang siber dapat digunakan untuk mengganggu, mengacau, hingga melumpuhkan infrastruktur krisis suatu negara. Kementerian Pertahanan sebagai *leading sector* pertahanan Indonesia juga masih rentan terhadap serangan siber yang terus berevolusi seiring perkembangan teknologi. Oleh karena itu risiko tersebut perlu dikelola dengan menerapkan manajemen risiko pertahanan siber melalui pendekatan kualitatif dengan desain penelitian fenomenologi. Melalui metode wawancara, observasi dan studi dokumentasi, data yang diperoleh dianalisis dalam empat tahapan, yaitu: pengumpulan data, kondensasi data, penyajian data, dan penarikan kesimpulan. Implementasi kebijakan yang diterapkan oleh Pusat Pertahanan Siber (Pushansiber) Kementerian Pertahanan masih perlu ditingkatkan terkait dengan komunikasi, sumber daya manusia, disposisi, dan struktur birokrasi. Hambatan ditemukan pada masih kurangnya jumlah personil yang dimiliki saat ini, terbatasnya anggaran, dan belum adanya *Standard Operational Procedure* (SOP) yang dimiliki oleh Pushansiber. Pushansiber perlu meningkatkan jumlah personil, menyegerakan angggaran, pembuatan SOP, dan penerapan standarisasi nasional.

Kata Kunci: Implementasi, Manajemen Risiko, Pertahanan Siber, Kementerian Pertahanan, Pertahanan Negara

Abstract *– The current globalization that is happening all over the world today has brought the world to the era of information and communication technology development so as to create an era that is completely digital or digital world. The development of the internet network is part of human culture that continues to evolve to find unlimited perfection in achieving ease of communication. From the perspective of cyber defense the use of the internet is also possible for negative or destructive purposes by those who have the ability. The facilities available in cyberspace can be used to disrupt, disrupt, and paralyze a country's crisis infrastructure. The Ministry of Defense as Indonesia's leading defense sector is also still vulnerable to cyber attacks that continue to evolve as technology develops. Therefore these risks need to be managed by implementing cyber defense risk management through a qualitative approach with a phenomenological research design. This study*

[1] Program Studi Manajemen Pertahanan, Fakultas Manajemen Pertahanan, Universitas Pertahanan
[2] Program Studi Manajemen Pertahanan, Fakultas Manajemen Pertahanan, Universitas Pertahanan
[3] Program Studi Manajemen Pertahanan, Fakultas Manajemen Pertahanan, Universitas Pertahanan

aims to see how the implementation of risk management related to cyber defense implemented by the Ministry of Defense Through interviews, observation and documentation studies, the data obtained were analyzed in four stages, namely: data collection, data condensation, data presentation, and drawing conclusions . Based on the results of the analysis it can be concluded that the implementation of policies implemented by the Ministry of Defense's Cyber Defense Center (Pushansiber) still needs to be improved related to communication, human resources, disposition, and bureaucratic structure. Obstacles are found in the current lack of personnel, limited budget, and the lack of Standard Operating Procedures (SOPs) owned by Pushansiber. Pushansiber needs to increase the number of personnel, hasten the budget, create SOPs, and implement national standards.

Key Words: Implementation, Risk Management, Cyber Defense, Ministry of Defense, National Defense

Pendahuluan

Arus globalisasi yang terjadi di seluruh dunia saat ini telah membawa dunia pada perkembangan teknologi informasi dan komunikasi sehingga menciptakan era yang serba digital atau digital world. Dalam hal ini, perkembangan teknologi komputer dan internet menjadi sarana baru bagi negara-negara di dunia untuk dimanfaatkan sebagai alat untuk melakukan berbagai penetrasi, pengaruh dan infiltrasi ke berbagai negara sehingga sangat mendorong dunia pada perkembangan yang kompleks, beragam dan majemuk.[4] Perkembangan pesat dari teknologi informasi dan komunikasi ini menciptakan ketergantungan yang sangat besar terhadap aktivitas kehidupan masyarakat. Perkembangan teknologi informasi yang mencakup teknologi komunikasi dengan menggunakan jaringan internet menjadikan interaksi antar manusia semakin bebas tanpa dibatasi ruang dan waktu.

Perkembangan jaringan internet merupakan bagian dari budaya manusia yang terus berevolusi mencari kesempurnaan tanpa batas dalam mencapai kemudahan dalam berkomunikasi. Interconnection Networking (Internet) mulai dikembangkan pada 1969 oleh Departemen Pertahanan Amerika Serikat (US Department of Defense) melalui proyek bernama Advanced Research Project Agency Network (ARPANET) dengan tujuan merancang dan membuat jaringan komputer yang tersebar namun saling terkoneksi satu dengan yang lain dan terpusatnya sebuah informasi hanya dalam satu station, sehingga apabila terjadi perang maka data dan informasi

[4] Adi Joko Purwanto, "Peningkatan Anggaran Militer Cina dan Implikasinya terhadap Keamanan di Asia Timur", SPEKTRUM: Jurnal Pertahanan dan Bela Negara, Vol. 7, 2010.

dapat cepat dipindahkan dari satu station ke station lain dan tidak mudah dihancurkan.[5]

Semakin luas dan meningkatnya pemanfaatan teknologi informasi dan komunikasi (TIK) melalui jaringan internet menjadikan Indonesia sebagai negara ke 5 pengguna internet aktif di dunia setelah China, India, Amerika Serikat dan Brazil, hal ini dapat menyebabkan meningkatnya ancaman seperti upaya membobol kerahasiaan data, membajak informasi pada website, merusak sistem elektronik seperti virus, malware dan ransomware dan perbuatan yang dapat merugikan dan melawan hukum lainnya (Permenhan No 82 Tahun 2014).

Sedangkan berdasarkan hasil studi Polling Indonesia yang bekerja sama dengan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2018, dari total 264 juta jiwa penduduk Indonesia sebanyak 171,17 juta jiwa atau sekitar 64,8 persen penduduk Indonesia telah terhubung dengan Internet.[6] Hal ini membuktikan bahwa perkembangan teknologi dan informasi telah merebak hampir kesemua kalangan. Perkembangan teknologi informasi dan komunikasi telah mampu menghilangkan hambatan geografis yang berimbas pada semakin meningkatnya bentuk ancaman terhadap pertahanan dan kedaulatan sebuah negara. Ancaman global dari kemajuan teknologi ini tidak hanya mengancam aspek kehidupan manusia, seperti ekonomi, politik, sosial, dan budaya, tapi juga menyerang instansi strategis pemerintah dan militer.

Fenomena ruang siber menggambarkan sebuah realitas bahwa aktifiktas kegiatan masyarakat modern saat ini sudah saling terkoneksi melalui ruang siber dan internet. Dari perspektif pertahanan siber (cyber defense) pemanfaatan internet juga dimungkinkan untuk tujuan negatif atau destruktif oleh pihak-pihak yang mempunyai kemampuan. Fasilitas yang tersedia di internet dapat digunakan untuk mengganggu, mengacau, hingga melumpuhkan infrastruktur krisis suatu negara.[7]

[5] Sutrisno, S.P, "Urgensi Komando Pertahanan Siber *(Cyber Defense Command)* dalam Menghadapi Peperangan Asimetris". Jurnal Defendonesia. Volume 1 Nomor 2, 2016

[6] Fajar S.I. Yudha dan Erwin Gunadhi, "Risk Assessment Pada Manajemen Risiko Keamanan Informasi Mengacu Pada British Standard ISO/IEC 27005 Risk Management", Jurnal Algoritma Sekolah Tinggi Teknologi Garut, Vol.13, 2016, hlm.333-340.

[7] Rudy Gemilang Gultom, Komunikasi Personal 14 Januari 2019

Ghemaoti mengatakan bahwa perkembangan teknologi informasi memberikan perubahan signifikan mengenai konsep keamanan.[8] Kini ruang interaksi tidak bisa hanya dibatasi secara fisik (*physic*) tapi juga meluas ke dunia maya (*cyber*). Konsekuensinya adalah negara harus beradaptasi dengan perkembangan ini. Hal ini akan menimbulkan pola ancaman baru yang harus dihadapi negara, yaitu ancaman siber. Ancaman dan serangan siber dapat dilakukan oleh pelaku yang mewakili pemerintah (*State Actors*) atau non pemerintah (*Non State Actors*), sehingga pelaku bisa bersifat perorangan, kelompok, golongan, organisasi, atau bahkan sebuah negara.

Dapat dibayangkan jika ada suatu divisi pasukan yang ahli komputer dan jaringan yang kemudian menggunakan keahliannya untuk mengoperasikan dan membajak jaringan komputer fasilitas-fasilitas publik seperti situs-situs pemerintah, pangkalan militer, perbankan, jaringan telekomunikasi, infrastruktur dan layanan transportasi. Tentunya hal ini akan menimbulkan kekacauan dan kerugian dari berbagai kalangan.

Gambaran tersebut merupakan contoh dampak yang diakibatkan oleh serangan siber yang bisa lebih menghancurkan dan mengacaukan dibanding serangan fisik. Banyak definisi tentang serangan siber, namun dalam Permenhan nomor 82 tahun 2014 tentang Pedoman Pertahanan Siber dijelaskan bahwa serangan siber *(cyber attack)* adalah adalah segala bentuk perbuatan, perkataan, pemikiran baik yang dilakukan dengan sengaja maupun tidak sengaja oleh pihak mana pun, dengan motif dan tujuan apa pun, yang dilakukan di lokasi mana pun, yang disasarkan pada sistem elektronik atau muatannya (informasi) maupun peralatan yang sangat bergantung pada teknologi dan jaringan dalam skala apa pun, terhadap obyek vital maupun nonvital dalam lingkup militer dan nonmiliter, yang mengancam kedaulatan negara, keutuhan wilayah dan keselamatan bangsa.

Serangan siber dapat menyerang setiap negara, beberapa kasus serangan siber berskala besar pernah tercatat di dunia, seperti: serangan *Titan Rain* tahun 2003 yang menyerang institusi penting di Amerika seperti *National Aeronautics and*

[8] D. Triwahyuni dan T.A. Wulandari, "Strategi Keamanan Cyber Amerika Serikat", Jurnal Ilmu Politik dan Komunikasi, Vol.6, No.1, 2016.

Space Administration (NASA) dan *Lockheed Martin*; lumpuhnya insfrastruktur kritis nasional di Estonia pada 2007 dan Georgia pada 2008; serangan terhadap Pusat Komando Amerika Serikat tahun 2008; serangan *spynet (Ghostnet)* yang merupakan program pencurian data oleh pemerintah China terhadap 103 negara pada 2008; operasi *Aurora* pada 2009 yang berhasil menyerang perusahaan besar seperti *Google* dan *Adobe System*; serangan *Stuxnet* pada tahun 2010 yang melumpuhkan pembangkit nuklir Bushwer; serangan *Flame* pada 2012 yang menyerang jaringan komputer yang menangani sektor minyak Iran; insiden *cyber attack* terhadap data perusahaan *Saudi Aramco Oil Company* di Saudi Arabia pada Agustus 2012; insiden *panama papers* pada April 2016, *Ransomware WannaCry* pada Mei 2017 serta masih banyak kasus kasus serangan siber dalam skala global lain.[9]

Negara Indonesia tidak lepas dari serangan siber, Indonesia pernah mengalami beberapa kali serangan siber, beberapa diantaranya seperti: pada 2010, Symantec sebagai produsen Antivirus Norton, mengumumkan bahwa Indonesia berada di urutan kedua setelah Iran di antara 10 negara yang mengalami serangan *worm Stuxnet*; Serangan siber *Ransomware WannaCry* pada Mei 2017 yang menyebabkan gangguan pada perusahaan dan rumah sakit di lebih dari 150 negara termasuk Indonesia;[10] Selain itu, salah satu situs resmi unit kerja Kementerian Pertahanan Republik Indonesia (Kemhan RI) dibobol oleh hacker, yakni website milik Direktorat Jenderal Potensi Pertahanan (Ditjen Pothan) yang mengalami perubahan laman yang disebut *defacing*. Situs Ditjen Pothan tersebut dibobol oleh CVT (*Cyber Vampire Team*) pada 2018.[11] Selain website resmi milik Kementerian Pertahanan, website resmi milik Kementerian Dalam Negeri (Kemendagri) juga pernah diretas oleh hacker pada September 2019, sebagai bentuk aksi protes terhadap diterbitkannya revisi Undang-Undang Komisi Pemberantasan Korupsi (KPK).

[9] Rudi Gemilang Gultom. Cyber Warfare Sudah Siapkah Kita Menghadapinya. (Bogor: Unhan Press, 2019)

[10] Nur Khalimatus Sa'diyah, "*Rekontruksi pembentukan nasional cyber defense sebagai upaya mempertahanakan kedaulatan negara.*" Jurnal Perspektif, Volume XXI no 3, 2017, Pp 168-187.

[11] Inue Rahmawati "*Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) dalam Peningkatan Cyber Defense.*" Jurnal Pertahanan dan Bela Negara. Vol 7, No.2, 2017, pp 51-66.

Dalam beberapa tahun terakhir juga terjadi perang siber antara Indonesia dengan Malaysia. Saling susup antara hacker kedua negara mewarnai perseteruan ini. Aksi ini biasanya terjadi ketika muncul konflik politik ataupun persaingan kedua negara. Meskipun tidak melibatkan pemerintah kedua negara, namun aksi para hacker ini menyerang fasilitas siber milik pemerintah Malaysia maupun Indonesia.

Kasus lain dari kejahatan cyber adalah kejahatan dalam bentuk Social Engineering. Dalam dokumen yang dibocorkan Whistleblower Edward Snowden, mantan kontraktor National Security Agency (NSA) Amerika Serikat yang dimuat oleh The Guardian dan ABC pada November 2013, Presiden ke-6 RI Susilo Bambang Yudhoyono (SBY) beserta wakil presiden Boediono dan beberapa jajaran di lingkungan kepresidenan pernah disadap oleh pemerintah Australia pada tahun 2009. Dalam dokumen tersebut tertulis bahwa intelijen elektronik Australia (Defence Signals Directorate/DSD) melacak kegiatan SBY melalui telepon genggam pada Agustus 2009, hal ini merupakan upaya pemetaan intelijen Australia untuk mengikuti peluncuran teknologi 3G di Indonesia dan seluruh Asia Tenggara. Dalam halaman lain berjudul "Indonesian President Voice Events", yang ditulis BBC disebutkan adanya dugaan memata-matai call data records (CDR) atau daftar rekaman panggilan oleh intelijen Australia terhadap kepala negara Indonesia.[12]

Berdasarkan laporan pemantauan keamanan internet Badan Siber dan Sandi Negara (BSSN) mencatat terjadi 232.447.974 serangan siber ke Indonesia selama tahun 2018. Menurut Anton Setiawan selaku Direktorat Proteksi Ekonomi Digital BSSN, dari serangan tersebut nyaris setengahnya merupakan serangan *malware*. Peningkatan serangan yang terjadi setiap tahun ini sebagai akibat dari semakin canggihnya serangan yang dikembangkan oleh aktor kriminal siber. Selain itu, sekitar 60 sampai 70 persen yang menjadi sasaran dari serangan siber adalah sektor publik. Situs pemerintah dengan domain *.go.id* menjadi sasaran empuk dengan *port 123* menjadi *port* yang paling sering diserang.[13]

[12] Riz, "Snowden: Ponsel SBY Disadap Australia", dalam Liputan 6: https://www.liputan6.com/ global/read/748895/ snowden-ponsel-sby-disadap -australia, 18 November 2013, diakses pada 15 Agustus 2019.

[13] CNN Indonesia "*BSSN: 232,45 Juta serangan siber serbu indonesia di 2018.*" Dalam CNN Indonesia: https://www.cnnindonesia. com/ teknologi/ 20181107155049-185-344721/kemenhan-

Kejadian-kejadian tersebut membuktikan bahwa Indonesia masih rentan terhadap serangan siber. Dampak yang muncul akibat serangan siber dapat berupa kerusakan sistem, pencurian informasi, manipulasi informasi atau perangkat, penyebaran informasi, dan lain-lain.

Di beberapa negara, pertahanan siber diterapkan di semua sektor, terutama yang memiliki data/informasi yang bersifat strategis atau kritis. Sektor strategis tersebut dapat diilustrasikan oleh gambar berikut, Pada gambar diatas dapat diketahui bahwa sektor strategis yang dimaksudkan dapat berupa sektor Pemerintah, Energi dan Sumber Daya Mineral, Transportasi, Jasa keuangan, Kesehatan, Teknologi Informasi dan Komunikasi, Pangan, Pertahanan, Industri Pertahanan dan sektor strategis lainnya.

Kementerian Pertahanan sebagai leading sector pertahanan Indonesia juga masih rentan terhadap serangan siber yang terus berevolusi seiring perkembangan teknologi. Oleh karena itu risiko tersebut perlu dikelola dengan menerapkan manajemen risiko pertahanan siber di Kementerian Pertahanan untuk mendukung pertahanan negara.

terima-80-ribu-serangan-hacker-tiap-hari, diakses pada 15 Agustus 2019

Metode Penelitian

Metode kualitatif dengan pendekatan fenomenologi sangat diperlukan dalam hubungannya dengan analisis terhadap masalah yang diteliti, sehingga batasan, lingkup, latar belakang dan signifikasinya tampak jelas. Paper ini merupakan hasil penelitian lapangan yang mengkaji implementasi manajemen risiko pertahanan siber Kementerian Pertahanan untuk mendukung pertahanan negara. Data-data yang diperoleh kemudian dikondensasi dan dianalisis menggunakan teknik analisis deskripsi kualitatif guna mendapatkan titik temu dalam penelitian ini.

Hasil dan Pembahasan

1. Gambaran Umum Pusat Pertahanan Siber Kementerian Pertahanan

Pusat Pertahanan Siber (Pushansiber) merupakan unsur pelaksana tugas dan fungsi Badan Instalasi Strategis Pertahanan (Bainstrahan) Kementerian Pertahanan (Kemhan). Pushansiber dipimpin oleh Kepala Pusat Pertahanan Siber (KaPushansiber). Pushansiber berlamat di Jl. RS Fatmawati No.1, RT.06/RW.06, Pondok Labu, Kec. Cilandak, Kota jakarta Selatan, Daerah Khusus Ibukota Jakarta.

Dalam melaksanakan tugas sebagaimana dimaksud dalam Peraturan Menteri Pertahanan Republik Indonesia pasal 1177 Nomor 14 Tahun 2019 Tentang Organisasi dan Tata Kerja Kementerian Pertahanan, Pushansiber menyelenggarakan fungsi sebagai berikut:

a. Penyusunan kebijakan teknis, program dan anggaran di bidang tata kelola, kerja sama, operasi, dan jaminan keamanan pertahanan siber;
b. Pelaksanaan tata kelola, kerja sama, operasi, dan jaminan keamanan pertahanan siber;
c. Pemantauan, evaluasi, pengendalian dan pelaporan di bidang tata kelola, kerja sama, operasi, dan jaminan keamanan pertahanan siber;
d. Pembentukan Computer Emergency Response Team (CERT) dalam rangka merespon serangan siber, serta pemantauan dan evaluasi dalam setiap pelaksanaan tugas CERT; dan
e. Pengelolaan ketatausahaan dan kerumahtanggaan pusat.

Pegawai Pushansiber adalah Pegawai Negeri Sipil (PNS), prajurit Tentara Nasional Indonesia (TNI), dan tenaga kontrak yang ditugaskan di Kemhan. Adapun struktur organisasi Pushansiber terdiri atas tiga bidang yakni:

a. Bidang tata kelola dan kerja sama yang bertugas menyusun tata kelola dan kerjasama pertahanan siber meliputi tata laksana, kerjasama, perencanaan, implementasi dan pemeliharaan siber;
b. Bidang operasi siber berfungsi
    1) Menyiapkan penyusunan kebijakan teknis di bidang operasi siber meliputi monitoring, analisis dan pelaporan ancaman siber, penindakan, digital forensik dan pemulihan;
    2) Melaksanakan operasi siber meliputi monitoring, analisis dan pelaporan ancaman siber, penindakan, digital forensik dan pemulihan;
    3) Pemantauan, evaluasi, pengendalian dan pelaporan di bidang operasi siber; dan
    4) Pembentukan Computer Emergency Response Team (CERT) dalam rangka merespon serangan siber, serta pemantauan dan evaluasi

dalam setiap pelaksanaan tugas CERT.

c. Bidang penjamin keamanan bertugas melaksanakan penjamin keamanan pertahanan siber dari ancaman eksternal.

2. Implementasi Manajemen Risiko Pertahanan Siber di Kementerian Pertahanan

Pertahanan siber merupakan mekanisme pertahanan jaringan komputer yang menyangkut reaksi terhadap tindakan dan perlindungan terhadap infrastruktur penting, serta jaminan terhadap informasi yang dimiliki oleh suatu organisasi atau entitas pemerintahan. Pada dasarnya konsep pertahanan siber berfokus pada tindakan pencegahan, pendeteksian dan penanggulangan serangan siber secara tepat, hingga tidak ada infrastruktur atau informasi yang akan mengalamai kerusakan[14].

Implementasi kebijakan merupakan pelaksanaan keputusan kebijaksanaan dasar, biasanya dalam bentuk undang-undang, namun dapat pula berbentuk perintah-perintah atau keputusan-keputusan eksekutif yang penting atau keputusan badan peradilan. Lazimnya, keputusan tersebut mengidentifikasikan masalah yang ingin diatasi, menyebutkan secara tegas tujuan atau sasaran yang ingin dicapai dan berbagai cara untuk menstrukturkan atau mengatur proses implementasinya.[15]

Implementasi merupakan perluasan aktivitas yang saling menyesuaikan proses interaksi antara tujuan dan tindakan yang untuk mencapainya memerlukan jaringan pelaksana, dan birokrasi yang efektif[16].

Dalam implementasi kebijakan akan selalu ada faktor-faktor pendukung dan penghambat dari suatu kebijakan, baik yang ada dari dalam maupun luar. George C. Edward III dalam teorinya, mengemukakan empat faktor yang menentukan keberhasilan suatu kebijakan, yaitu Komunikasi, Sumber Daya, Disposisi dan Struktur Birokrasi. Proses ini merupakan sebuah performa dari suatu kebijakan yang pada dasarnya dilakukan untuk meraih kinerja implementasi kebijakan publik yang baik,

[14] Darko Galinec, Darko Moznik, dan Boriz Guberina, "*Cybersecurity and Cyber Defense: National Cyber Strategich Approach*", Jurnal Automatika. Vol. 58, No. 3, 2017, pp. 273-286.",

[15] H. Daniel Mazmanian dan Paul A. Sabatier, Implementation and Public Policy, (New York: Harper Collins, 1983).

[16] Guntur Setiawan, Implementasi dalam Birokrasi Pembangunan, (Jakarta: Rajawali Press, 2004)

yang berlangsung dalam hubungan berbagai faktor.[17]

a. Komunikasi (*Communication*)

Komunikasi sangat menentukan keberhasilan pencapaian tujuan dari implementasi kebijakan. Implementasi dapat terjadi apabila para pembuat keputusan sudah mengetahui apa yang akan mereka kerjakan. Pengetahuan atas apa yang akan dikerjakan baru dapat berjalan apabila komunikasi berjalan dengan baik, sehingga setiap keputusan kebijakan dan peraturan pada implementasi harus ditransmisikan melalui komunikasi kepada bagian yang tepat. Selain itu, kebijakan yang dikomunikasikan harus tepat, akurat dan konsisten. Komunikasi atau pentransmisian informasi diperlukan agar para pembuat keputusan dan para implementer semakin konsisten dalam melaksanakan setiap kebijakan yang akan diterapkan.[18]

Cara yang baik dalam menjelaskan sebuah komunikasi adalah dengan memenuhi lima unsur yang terdapat dalam komunikasi,[19] unsur-unsur tersebut adalah:

1) Penyampai pesan, yaitu seseorang yang memberikan pesan kepada penerima pesan. Dalam hal ini penyampai pesan harus dapat memahami apa yang ingin disampaikan kepada penerima pesan.
2) Pesan, yaitu pesan yang ingin disampaikan haruslah pesan yang mudah dipahami dan memiliki makna yang mudah dipahami agar penerima pesan mengerti akan apa yang disampaikan oleh penyampai pesan.
3) Media, yaitu sarana atau alat guna menyampaikan pesan. Dalam hal ini sebagai jembatan antara penyampai pesan dan penerima pesan.
4) Penerima pesan, yakni pihak yang dituju oleh penyampai pesan. Sebuah komunikasi dikatakan berhasil jika pesan yang disampaikan sampai dan dapat diterima dengan baik oleh penerima pesan.

Komunikasi yang dijalin Kemhan baik secara Internal maupun eksternal antara

[17] George C. Edward III, Impementing Public Police, (Washington: Congressional Quarterly Press, 1980).
[18] Ibid.
[19] H. Lasswell, The Sructure and Function of Communication in Society, 1960.

pemangku kepentingan di dalam maupun di luar kemhan masih belum optimal. Komunikasi internal yang dilakukan Pushansiber dalam mendukung aspek komunikasi ini adalah dengan bertatap muka langsung antara personil dan pimpinan yang berkepentingan. Sedangkan komunikasi eksternal dilakukan ke pihak luar melalui surat menyurat antar instansi dan menggunakan komunikasi elektronik seperti E-mail. Pushansiber dan BSSN tidak berada dalam satu garis komando, sehingga koordinasi terkait siber dilakukan melalui surat menyurat dan E-mail. Sedangkan untuk kegiatan FGD dan *Cyber Drill Test* dari BSSN hanya diikuti oleh beberapa delegasi Pushansiber.

Berkaitan dengan komunikasi ini Pushansiber juga menerapkan prinsip manajemen pertahanan berupa Fungsi Koordinasi. Tugas koordinasi berkaitan dengan penyatuan dan penggabungan usaha semua bagian organisasi atau semua anggota kelompok kerja, dalam pencapaian tujuan bersama yang didefinisikan dalam tahap perencanaan. Ini melibatkan pengintegrasian berbagai bagian yang terlibat dalam tugas-tugas, memesan dan menghubungkan berbagai aktivitas yang perlu dilakukan, dan menjaga komunikasi yang efektif.[20]

Dalam menyikapi kebijakan pembangunan pertahanaan siber yang efektif di lingkungan pertahanan, Kemhan khususnya Pushansiber saling berkoordinasi dalam merumuskan kebijakan pertahanan siber yang kuat di lingkungan Kementerian pertahanan, tentunya dalam pembuatan kebijakan tersebut melibatkan orang orang yang yang ahli dibidangnya. Pada tataran internal, koordinasi dilakukan secara langsung sesuai dengan substansi dan pokok persoalan yang akan dilakukan maupun melalui kegiatan rapat-rapat yang mengundang satuan kerja terkait di lingkungan Kemhan. Pada tataran eksternal, koordinasi dilakukan melalui kegiatan rapat antar kementerian atau lembaga lain terkait substansi yang dibahas maupun dengan kegiatan seminar yang melibatkan K/L lain terkait guna memperoleh masukan yang konstruktif untuk kepentingan bersama. Koordinasi baik di tataran internal maupun eksternal Kemhan dilaksanakan melalui media kegiatan Rapat Koordinasi Pimpinan dan Rapat Kerja.

[20] Laura R. Cleary dan Tery McConville, (eds.), Managing Defense in A Democracy, (London: Routledge, 2006).

Arus koordinasi telah diatur oleh pemerintah dengan menjadikan BSSN sebagai leading sector pertahanan siber. Pengelolaan siber oleh BSSN melingkupi siber milik Polri, Kemhan, Kejaksaan, TNI, Kominfo dan kementerian/lembaga lainnya. Olehnya, BSSN harus memiliki Sistem Pusat Komando dan Kendali Nasional di bidang siber. Sedangkan lembaga lainnya mengurus satu bidang yang berbeda, seperti Pushansiber di lingkungan Kemhan, Satsiber di lingkungan TNI, Polri di bidang *cyber crime*, dan lain sebagainya.

b. Sumber Daya (*Resources*)

Faktor sumber daya memiliki peran yang sangat penting dalam implementasi. Apabila suatu implementasi telah memiliki ketentuan dan aturan yang jelas, namun jika sumber daya yang akan melaksanakan implementasi tidak dapat melakukan kebijakan secara efektif maka implementasi yang tadinya berjalan efektif menjadi tidak efektif. Sumber daya yang dimiliki akan menentukan berhasil tidaknya implementasi bila sumber daya tersebut mampu untuk memfasilitasi pelaksanaan implementasi secara efektif.

Pushansiber dalam melaksanakan poin tersebut telah melaksanakan beberapa poin dengan sangat baik untuk mendukung pertahanan siber di kementerian pertahanan. Faktor sumber daya yang dimiliki Pushansiber meliputi sumberdaya manusia, sumberdaya anggaran, dan sumberdaya fasilitas.

1) Sumber Daya Manusia

Edward III dalam Widodo (2010:98) menyatakan bahwa mungkin sumber daya yang paling terpenting dalam implementasi kebijakan adalah sumber daya manusia.[21] Sumber daya manusia adalah pilar penyangga utama sekaligus penggerak roda organisasi dalam usaha mewujudkan visi dan misi organisasi.[22]

Agar dapat melaksanakan tugasnya dengan baik, maka ada beberapa persyaratan umum yang harus diperhatikan oleh lembaga pertahanan siber dalam pengembangan SDM seperti dalam hal rekrutmen SDM. Proses rekrutmen harus melewati uji kesiapan mental melalui tes psikologi agar sesuai dengan

[21] Joko Widodo, Analisis Kebijakan Publik, (Malang: Bayumedia, 2010), hlm.100-101.
[22] S. Martoyo, Manajemen Sumber Daya Manusia (Edisi Kedelapan), (Yogyakarta: BPFE, 2003), hlm.3.

profil dari SDM untuk pertahanan siber. SDM terpilih harus memiliki kompetensi sesuai dengan kebutuhan, dalam hal pengetahuan dan ketrampilan sesuai penempatan dan penugasan dalam pertahanan siber serta terjaminnya pembinaan karier SDM yang bersangkutan. Untuk tugas-tugas khusus yang bersifat rahasia dan strategis , SDM terpilih harus memiliki status kepegawaian yang tidak menyalahi prinsip-prinsip organisasi pertahanan, khususnya untuk tugas yang bersifat ofensif atau dalam kondisi perang siber.[23]

Sumber daya manusia yang dimiliki Pushansiber saat ini berjumlah kurang lebih 100 orang yang terdiri dari PNS, TNI dan tenaga kontrak. Jumlah ini masih kurang dari jumlah yang dibutuhkan. Sumber daya manusia sangat berpengaruh terhadap keberhasilan implementasi, kurangnya sumber daya menyebabkan implementasi akan berjalan lambat. Sedangkan untuk rekrutmen personil baru, Pushansiber masih menunggu perekrutan dari pemerintah.

Sedangkan dari sisi kuailtas, personil yang dimiliki saat ini cukup mumpuni untuk bergerak di bidang pertahanan siber, khususnya dalam pengamanan jaringan. Hanya saja kendala yang dimiliki oleh personil ini adalah sertifikasi. Sebagian besar personil yang dimiilki masih belum memiliki sertifikasi, hal ini dikarenakan oleh keterbatasan anggaran yang dimiliki oleh instansi. Selain itu personil juga masih terkendala dalam penguasaan bahasa Inggris.

Berdasarkan hasil analisis diatas dapat disimpulkan bahwa Pushansiber masih belum optimal terkait sumber daya manusia yang ada, hal ini dikarenakan kurangnya jumlah personil yang dimiliki. Kurangnya jumlah personil tersebut nantinya akn berpengaruh terhadap pelaksanaan implementasi pertahanan siber di kementerian Pertahanan. Selain itu terbatasnya jumlah personil yang memiliki sertifikasi, meskipun kualifikasi personil pushansiber dikatakan

[23] Permenhan no 82 tahun 2014 tentang Pedoman Pertahanan Siber

telah mampu untuk melakukan berbagai pengamanan jaringan di lingkungan Kementerian Pertahanan, dengan tidak adanya sertifikasi sesuai bidangnya hal ini akan menjadi kendala terkait kemampuan masing masing personil yang ada. Selain itu keterbatasan kemampuan dalam berbahasa khususnya penggunaan Bahasa Inggris dalam dalam kegiatana pengamanan jaringan karena sebagian besar bahasa pengantar yang digunakan dalam ilmu komputer adalah Bahasa Inggris, dengan kurang dikuasainya kemampuan berbahasa oleh personil akan menurunkan kewaspadaan personil dalam pengamanan jaringan.

2) Sumber Daya Anggaran

Edward III menyatakan bahwa terbatasnya anggaran yang tersedia menyebabkan kualitas pelayanan yang seharusnya diberikan kepada masyarakat juga terbatas. Terbatasnya sumber daya anggaran akan mempengaruhi keberhasilan pelaksanaan kebijakan karena tidak bisa dilaksanakan dengan optimal.[24]

Anggaran berkaitan dengan kecukupan investasi atau modal-modal untuk menjamin terlaksananya program suatu kebijakan. Sebab dengan tanpa dukungan dari anggran yang memadai, kebijakan tidak akan berjalan dengan efektif dalam mencapai tujuan dan sasaran.

Sumber daya anggaran yang dimiliki oleh Pushansiber saat ini adalah sumber kendala terbesar. Dalam masalah sumber daya anggaran ini, ternyata Pushansiber belum memiilki anggaran yang berdiri sendiri. Hal ini dikarenakan Pushansiber baru berdiri selama dua tahun. Pushansiber dulunya merupakan pecahan dari Pusdatin kemhan. Untuk itu hingga saat ini anggaran yang ada masih merupakan limpahan dari Pusdatin hingga tahun 2018, sedangkan untuk 2019 anggran yang diterima sudah tidak ada. Hal ini didukung oleh pernyataan Kolonel Trisatya bahwa selama dua tahun berdirinya Pushansiber belum ada

[24] Joko Widodo, Analisis Kebijakan Publik, (Malang: Bayumedia, 2010), hlm.100-101.

anggaran, anggaran masih dilimpahkan dari Pusdatin sampai tahun 2018.

Anggaran sangat diperlukan untuk melatih atau mentraining personil. Bahkan pelatihan yang paling dasar seperti keamanan atau antivirus juga memerlukan anggaran.

3) Sumber Daya Fasilitas

Edward III menyatakan bahwa terbatasnya anggaran yang tersedia menyebabkan kualitas pelayanan yang seharusnya diberikan kepada masyarakat juga terbatas. Terbatasnya sumber daya anggaran akan mempengaruhi keberhasilan pelaksanaan kebijakan karena tidak bisa dilaksanakan dengan optimal.[25]

Menurut Richardus Eko Indrajid (2014) ada aspek aspek terkait lingkungan fisik yang harus benar benar diperhatikan oleh perusahaan untuk mendukung keamanan data, yaitu: Akses masuk organisasi, lingkungan sekitar organisasi, daerah pusat informasi, ruang server, area *workstation, wireless access points, fiksimili* dan media elektronik lainnya, entitas kendali akses, pengelolaan aset komputer, penyadapan, dan *remote akses*.[26]

Berdasarkan Permenhan No 82 Tahun 2014 tentang Pedoman Pertahanan Siber, kelembagaan pertahanan siber memerlukan dukungan teknologi/infrastruktur seperti: (1) Sarana prasarana gedung/lokasi pusat data, NOC, laboratorium dan fasilitas pendukung lainnya, (2) Pusat Data dan pusat pemulihan *(Disaster Recovery Center/ DRC)*, (3) Jaringan Data, (4) Aplikasi administrasi pertahanan siber, (5) Aplikasi khusus teknis pertahanan siber, (6) Teknologi khusus (Perangkat keras dan perangkat lunak pendukung kegiatan spesifik pertahanan siber)

Untuk lingkungan sekitar, kantor Pushansiber berada di area publik dan dekat dengan pasar tradisional. Hingaa saat ini masih belum terdukung fasilitas mess untuk personil Pushansiber. Gedung yang digunakan

[25] Ibid.

[26] Indrajit Ricardus Eko. (2014). *Konsep dan Strategi Keamanan Informasi di Dunia Cyber.* Yogyakarta: Graha Ilmu.

Pushansiber saat ini dulunya adalah gedung milik Pusdatin kemhan. Namun dengan adanya struktur organisasi baru, gedung ini akhirnya diserahkan ke Bainstrahan, dan dialihfungsikan kepada Pushansiber seperti saat ini. Kondisi bangunan untuk aktifitas organisasi cukup baik dengan banyak ruangan-ruangan tertutup. Kondisi gedung juga sudah tersusun dengan baik dan memiliki pembagian ruangan yang tertata dengan rapi. Seluruh ruangan khusus sudah terpasang kartu akses dan hanya orang-orang tertentu yang dapat masuk ke dalam ruangan tersebut.

Pushansiber juga didukung oleh laboratorium *Digital Forensik*, laboratorium *Malware*, laboratorium Simulasi, laboratorium Jaringan, laboratorium Elektronika, dan Data Center. Pushansiber bergerak di koor bisnis pengamanan jaringan, untuk itu Pushansiber telah didukung oleh tujuh sensor yang berada di tujuh tempat berbeda, yaitu: Merdeka Barat, Bintaro, Cawang, Tugu Tani, Pondok Labu, Salemba, dan Sentul. Sensor yang digunakan ada dua jenis, yakni IPS dan IDS sensor.

c. *Disposition* (Sikap/Komitmen)

Disposisi atau sikap dari pelaksana kebijakan menurut Edward III (1980) adalah faktor penting ketiga dalam pendekatan mengenai implementasi suatu kebijakan. Jika kebijakan ingin efektif, maka para pelaksana kebijakan tidak hanya harus mengetahui apa yang akan dilakukan tetapi juga harus memiliki kemampuan untuk melaksanakannya Salah satu faktor yang mempengaruhi implementasi kebijakan adalah sikap implementer. Jika implementer setuju dengan bagian-bagian isi dari kebijakan maka mereka akan melaksanakan dengan senang hati tetapi jika pandangan mereka berbeda dengan pembuat kebijakan maka proses implementasi akan mengalami banyak masalah. Sama halnya di Kemhan, di seluruh kementerian dan lembaga lain bahwa komitmen dan visi pemimpin menjadi sangat penting dalam menjalankan roda organisasi melalui program program yang telah direncanakan.

Dalam penerapan implementasi dari segi disposisi ini, Pushansiber juga sekaligus menerapkan fungsi pengarahan. Fungsi pengarahan dalam

manajemen pertahanan merupakan proses memotivasi, memimpin dan mempengaruhi orang dalam mencapai tujuan bersama dalam bidang pertahanan. Pengarahan membutuhkan rasa dan keterampilan organisasi, dan kapasitas kepemimpinan untuk memotivasi para bawahan melalui atmosfer kerja yang menyenangkan.

Kebijakan dan regulasi juga diperlukan untuk menjaga arah dari kegiatan-kegiatan pengembangan pembangunan dan penerapan pertahanan siber agar senantiasa sesuai dengan peraturan perundangan. Pada tingkatan operasional kebijakan regulasi berbentuk pedoman, petunjuk pelaksanaan, petunjuk teknis yang menjadi acuan utama bagi pertahanan siber. Tata cara perumusan penetapan dan penerapan kebijakan pertahanan siber mengikuti tata cara berdasarkan peraturan perundangan dan dilakukan dengan mempertimbangkan kebutuhan nasional, perkembangan situasi dan kondisi pertahanan siber serta perkembangan teknologi.

Berdasarkan Permenhan No 82 Tahun 2014 tentang Pedoman Pertahanan Siber, kebijakan operasional penyelenggaraan pertahanan siber berupa: Perencanaan Keamanan Informasi *(Information Security Planning)*, Tanggap Darurat *(Incident Response)*, Manajemen resiko TIK *(IT Risk Management)*, Pemulihan *(Disaster Recovery)*, Rehabilitasi dan Rekonstruksi *(Disaster Rehabilitation and Reconstruction)*, Manajemen Rekanan *(Vendor Management)*, Operasi Jaringan *(Network Operations)*, Keamanan Sistem dan Aplikasi *(System and Application Security)*, Kontrol Akses *(Access Control)*, Kontrol Perubahan *(Change Control)*, Keamanan Fisik *(Physical Security)*, Klasifikasi data, penanganan dan pemusnahan *(Data Classification, Handling, and Disposal)*, Keamanan personel *(Personnel Security)*, Akses sistem dan penggunaan baku *(System Access and Acceptable Use)*, Privasi daring *(Online Privacy)*, Pelatihan dan kesadaran keamanan *(Security Training and Awareness)*, Asesmen diri *(Self Assessment)*, Metrik dan pengukuran keamanan *(Security Metrics and Measurement)*, Komputasi bergerak *(Mobile Computing)*, Keamanan Nirkabel *(Wireless Security)*.

Dalam menindak lanjuti kebijakan yang telah dirumuskan, secara rutin Kemhan menyusun kebijakan pertahanan negara tahunan yang secara substansi berisi tentang visi, misi

pembangunan, tujuan dan sasaranstrategis, program agenda prioritas, serta pokok-pokok kebijakan. Kebijakan pertahanan negara tahunan merupakan secara direktif dari Menhan yang disampaikan kepada seluruh pimpinan Kemhan di setiap awal tahun. Pengarahan direktif inilah yang dijadikan sebagai acuan bagi seluruh Unit Organisasi Kemhan dalam menyelenggarakan programnya masing-masing. Hal ini merupakan gambaran bentuk pengarahan yang dilakukan pimpinan kepada unsur-unsur di bawahnya.

Pengarahan oleh pimpinan Pushansiber dilakukan dalam bentuk instruksi secara langsung, rapat-rapat terbatas maupun rapat koordinasi, serta melalui penjabaran dari peraturan dan keputusan yang diberlakukan. Berdasarkan hasil analisis tersebut dapat disimpulkan bahwa komitmen Pushansiber dalam hal pertahanan siber telah terpenuhi dengan baik.

Penanganan yang akan dilakukan oleh Pushansiber kedepannya adalah jika Pushansiber telah memiliki anggaran maka Pushansiber akan diaudit terlebih dahulu dari segi *people*, *procces*, dan *technology*. Bagaimana personil yang ada, proses yang berlangsung saat ini, hingga teknologi yang digunakan. Berdasarkan hasil audit tersebut Pushansiber akan mengambil tindakan. Apakah nanti masing masing personil harus memiliki sertifikasi termasuk CCNE, CCNP, Ethical Hacker, forensik dan lainnya sebagainya. Setelah itu akan diusulkan pelatihan untuk personil yang ada. Kemudian dari sisi prosesnya, karena Pushansiber masih belum memiliki *Standar Operational Procedure* (SOP), nantinya Pushansiber akan mengusulkan SOP, Pushansiber berencana membuat 32 SOP dimasing masing labolatorium. Setelah itu barulah nanti Pushansiber akan mengadopsi ISO 27001, ISO 27005, Cobit, Cosco, NIST dan lainnya, sedangkan dari sisi teknologi nanti akan diaudit, apakah teknologi yang digunakan saat ini masih relevan dengan perkembangan zaman, ataukah teknologi yang ada harus di *upgrade*.

d. Struktur Birokrasi

Struktur organisasi Pushansiber seperti sudah digambarkan dalam organisasi sebelumnya menunjukkan bahwa untuk Pushansiber dipimpin oleh Kapushansiber. Kebijakan tertinggi di Pushansiber berada di tangan Kepala Pushansiber Marsma TNI Raja H Manalu, yang membawahi tiga kepala bidang. Tiga Kepala Bidang tersebut adalah

Kepala Bidang Tata Kelola dan Kerjasama, Kepala Bidang Operasi Siber, dan Kepala Bidang Penjamin Keamanan. Koor bisnis dari Pushansiber adalah mengamankan jaringan Kementerian Pertahanan. Pushansiber sendiri adalah Subsatker, dengan satuan kerja Bainstrahan. Berdasarkan Permanhan No 14 tahun 2019 tentang Organisasi dan Tata Kerja Kementerian Pertahanan, Bainstrahan itu terdiri dari tiga subsatker, yaitu Pusat Informasi Strategis Pertahanan (Pusinfostrahan), Pusat Pengembangan dan Pengelolaan (Pusbangkelola), dan Pusat Pertahanan Siber (Pushansiber) yang masing masing dipimpin oleh setingkat Eselon dua. Pushansiber terdiri dari Kapus, dan tiga kepala bidang, Kabid Tata Kelola dan Kerjasama, Kabid Operasi Siber, dan Kabid Penjamin Keamanan. Ruang lingkup Pushansiber sangat kecil, hanya menangani sebatas jaringan di Kemhan saja.

Koor bisnis dari Pushansiber adalah pengamanan jaringan. Pengamanan jaringan yang dilakukan oleh Pushansiber berada pada sektor wilayah Kementerian Pertahanan. Namun hingga saat ini Badan Siber dan Sandi Negara (BSSN) sebagai regulator pertahanan siber di Indonesia belum mengeluarkan legalitas yang menyatakan bahwa Pushansiber bertanggung jawab terhadap sektor pertahanan yang lebih luas termasuk pengamanan jaringan di TNI dan Industri pertahanan lain.

Sebagai pengaman jaringan wilayah Kementerian Pertahanan Pushansiber juga bertanggung jawab mengamankan segala macam bentuk informasi yang dimiliki kementerian pertahanan, salah satunya adalah sistem informasi pertahanan negara yang berisi informasi mengenai kekuatan pertahanan negara Indonesia, kekuatan militer negara asing, hingga data personil kementerian pertahanan.

Semua data yang ada di Kementerian Pertahanan adalah data-data yang penting, namun ada data yang boleh di informasikan ke publik dan data yang tidak boleh di akses oleh publik. Sehingga data-data yang ada di Kementerian Pertahanan harus dilindungi, baik dilindungi secara Information Technology (IT) maupun secara legalitas (hukum).

Sesuai dengan Permenhan Nomor 14 tahun 2019 tentang Organisasi dan Tata Kerja Kemhan secara terinci telah dijelaskan bahwa organisasi disusun secara struktural berdasarkan eselonisasi dan struktur tugas yang diemban.

Tupoksi dari masing Unit Organisasi secara terperinci sudah mewadahi kebijakan Kemhan dalam pertahanan siber yang di lingkungan Kemhan.

Kesimpulan dan Rekomendasi

Implementasi manajemen risiko pertahanan siber di Kementerian Pertahanan dinilai masih kurang optimal terkait dengan keberhasilan implementasi kebijakan yang mencakup komunikasi, sumber daya, struktur birokrasi, dan disposisi. Dalam aspek komunikasi masih belum adanya hubungan kerjasama lebih lanjut antara Pusat Pertahanan Siber dengan instansi lain yang juga bergerak dalam hal penanganan siber. Dalam aspek sumber daya Pusat Pertahanan Siber (Pushansiber) masih terkendala jumlah personil, kualifikasi personil yang masih belum memiliki sertifikasi dan terbatasnya anggaran yang ada. Dalam aspek sikap/komitmen Pushansiber telah menunjukan sikap dan komitmen dalam upayanya sebagai organisasi yang bergerak dalam pengamanan jaringan di lingkungan Kemhan. Hanya saja dalam hal ini Pushansiber masih belum memiliki *Standard Operational Procedure* (SOP) terkait manajemen risiko.

Adapun rekomendasi dari penelitian ini, antara lain:

1. Untuk meningkatkan keberhasilan implementasi kebijakan terkait dengan pertahanan siber di Kementerian Pertahanan perlu ditingkatkan interaksi dan komunikasi yang lebih intensif antara Pusat Pertahanan Siber dengan instansi lain yang juga bergerak di bidang pengamanan jaringan, terutama Badan Siber dan Sandi Negara (BSSN).
2. Untuk melaksanakan tugas dalam hal penanganan siber dilingkungan kementerian Pertahanan, Pushansiber perlu meningkatkan kapabilitas personil yang ada, meliputi: memastikan penguasaan Bahasa Inggris personil dalam kategori baik, meningkatkan jumlah personil yang dimiliki pada angka yang optimal, menjalankan program pendidikan dan pelatihan secara berskala, dan memastikan setiap personil memiliki sertifikasi di bidang kerjanya masing-masing.
3. Kementerian Pertahanan perlu menyiapkan dan menyegerakan anggaran yang mencukupi untuk tiap satuan kerja yang ada di lingkungan Pushansiber sesuai

dengan risiko ancaman yang dihadapi.

4. Pushansiber harus segera merumuskan *Standard Operational Procedure* (SOP) yang berperan sebagai petunjuk bagi personil satuan kerja dalam melaksanakan tugasnya.
5. Kementerian pertahanan khususnya pushansiber harus menerapkan standarisasi yang berkaitan dengan risiko serangan siber, kerangka kemanan informasi tersebut dapat menggunakan standari yang dikeluarkan oleh: *International Organization for Standardization* (ISO), *National Institute of Standards and Technology* (NIST) 800-30, *Control Objective for Information and Related Technology* (COBIT), *Operationally Critical Threat, Asset, and Vulnerability Evaluation* (OCTAVE).

Daftar Pustaka

Buku

Cleary, Laura R. dan McConville, Tery. (eds.). (2006). *Managing Defense in A Democracy*. London: Routledge.

Edward III, George C. (1980). *Impementing Public Police*. Washington: Congressional Quarterly Press.

Gultom, Rudy. (2019). *Cyber Warfare Sudah Siapkan Kita Menghadapinya.* Bogor: Unhan Press

Indrajid, Ricardus Eko. (2014). *Konsep dan Strategi Keamanan Informasi di Dunia Cyber.* Yogyakarta: Graha Ilmu.

Lasswell, H. (1960). *The Sructure and Function of Communication in Society*.

Martoyo, S. (2003). *Manajemen Sumber Daya Manusia (Edisi Kedelapan)*. Yogyakarta: BPFE.

Mazmanian, H. Daniel dan Sabatier, Paul A. (1983). *Implementation and Public Policy.* New York: Harper Collins.

Setiawan, Guntur. (2004). *Implementasi dalam Birokrasi Pembangunan.* Jakarta: Rajawali Press

Widodo, Joko. (2010). *Analisis Kebijakan Publik*. Malang: Bayumedia.

Jurnal

Fajar S.I. Yudha dan Gunadhi, Erwin. (2016). *Risk Assessment Pada Manajemen Risiko Keamanan Informasi Mengacu Pada British Standard Iso/Iec 27005 Risk Management. Jurnal Algoritma Sekolah Tinggi Teknologi Garut*. Vol.13. hlm.333-340.

Galinec, Darko, Darko Moznik dan Boris Guberina. (2017). *Cybersecurity and Cyber Defense: National Cyber Strategich Approach*. Automatika. Vol. 58, No. 3. pp. 273-286.

Sa'diyah, Nur Khalimatus. (2016). *Rekontruksi pembentukan nasional cyber defense sebagai upaya mempertahanakan kedaulatan negara.* Perspektif. Volume XXI no 3. Pp 168-187.

Purwanto, Adi Joko. (2010). *Peningkatan Anggaran Militer Cina dan Implikasinya terhadap Keamanan di Asia Timur. SPEKTRUM: Jurnal Pertahanan dan Bela Negara*. Vol. 7.

Rahmawati, Inue. (2017). *Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) dalam Peningkatan Cyber Defense*.

Jurnal Pertahanan dan Bela Negara. Vol 7, No.2, pp 51-66.

Sutrisno, SP. (2016). *Urgensi Komando Pertahanan Siber (Cyber Defense Command) dalam Menghadapi Peperangan Asimetris.* Jurnal Defendonesia. Volume 1 Nomor 2.

Triwahyuni, D. dan Wulandari, T.A. (2016). *Strategi Keamanan Cyber Amerika Serikat. Jurnal Ilmu Politik dan Komunikasi*. 6(1).

Website

Riz, "Snowden: Ponsel SBY Disadap Australia", dalam Liputan 6: https://www.liputan6.com/global/read/748895/ snowden-ponsel-sby-disadap-australia, 18 November 2013, diakses pada 15 Agustus 2019.

CNN Indonesia. 2019. *BSSN: 232,45 Juta serangan siber serbu indonesia di 2018.* CNN Indonesia. From https://www. cnnindonesia.com/ teknologi/20190426125843-192-389855/bssn-23245-juta-serangan-siber-serbu-indonesia-di-2018 pada 19 desember 2019

Peraturan dan Dokumen Tertulis

Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber