PENGARUH KOMUNIKASI DAN SUMBER DAYA TERHADAP KEAMANAN INFORMASI DI BADAN CYBER OPERATION CENTER PUSAT DATA DAN INFORMASI KEMENTERIAN PERTAHANAN REPUBLIK INDONESIA

Oleh

Ericka Novianandа[1], Freddy J Rumambi[2], Rayanda Barnas[3]

Universitas Pertahanan

ericka.novianandа@idu.ac.id

Abstract *– Cyber defense is intended to secure the confidentiality, integrity, and availability of important information for the country, national security, as well as securing Electronic System which is strategic or critical for the country. The Ministry of Defense of the Republic Indonesia is developing a Country Defense Information System based on providing a fast, accurate, and real time data and information in order to secure the decision making process. This research aims to determine the impact of communication and resources on information security at The Cyber Operation Center, Data and Information Center of Ministry of Defense of the Republic Indonesia. Every implementer needs to be aware that information security plays an important role in securing the country's strategic defense assets. This research reviews the implementation of George Edward III Implementation Theory that consists on Communication and Resources Variables. The hypothesis of this research is that there is a significant impact between communication and resources to Information Security. This research used quantitative method with 103 respondent samples, by using questionnaire to collect the data and statistical analysis using SPSS to analyze the data. The result of statistical analysis proves that there is 36,94% positive and significant impact between Communication to Information Security. There is 30,41% positive and significant impact between Resources to Information Security. There is 32,7% positive and significant impact between Communication and Resources to Information Security.*

Keyword *– Information Security, Communication, Resources, Implementation Police, Cyber Defense*

[1] Mahasiswa S2 Program Studi Manajemen Pertahanan, Cohort 8, Universitas Pertahanan

[2] Dosen Universitas Pertahanan

[3] Dosen Universitas Pertahanan

PENDAHULUAN

Pada era globalisasi saat ini atau sering dibilang abad informasi, telah mengubah pemahaman terhadap kekuatan atau kedaulatan dari suatu negara yang tadinya hanya dinilai dari kekuatan militer atau ekonomi yang dimiliki negara tersebut menjadi bergantung pada penguasaan dan pemanfaatan Teknologi dan Informasinya (TIK). Seiring dengan perkembangan TIK yang semakin pesat, menyebabkan setiap negara bergantung terhadap TIK baik dalam menjalankan roda pemerintahan maupun dalam rangka pelayanan kepada publik.

Di era cyber ini dengan terbukanya era *borderless*, keberadaan TIK mampu menghilangkan berbagai hambatan geografis yang berakibat dengan perkembangan teknologi informasi, berimbas pada semakin banyaknya bentuk ancaman terhadap keamanan *(national security)* dan kedaulatan sebuah negara. Ancaman keamanan *cyber* tidak lagi dipandang pada masalah teknis keamanan komputer semata melainkan mencakup aspek ideologi, politik, ekonomi, sosial, budaya dan keamanan nasional.[4] Oleh karena itu, sarana dan prasarana infrastruktur negara yang memanfaatkan TIK sangat penting untuk dilindungi.

Penguasaan dan pemanfaatan TIK yang salah akan menjadi ancaman jika negara tersebut tidak mampu memanfaatkan TIK secara baik, benar dan tepat guna. Semakin meluasnya dan meningkatnya pemanfaatan TIK khususnya melalui jaringan internet diiringi pula dengan meningkatnya aktivitas ancaman. Ancaman tersebut berupa upaya membobol kerahasiaan informasi, merusak sistem elektronik dan berbagai perbuatan melawan hukum lainnya.[5] Oleh sebab itu pertahanan siber *(cyber defense)* sangat diperlukan dalam sebuah negara.

TIK sebagai salah satu unsur strategis dalam mendukung penyelenggaraan pertahanan dan keamanan sudah selayaknya mendapatkan perhatian lebih. Terlebih lagi dalam beberapa tahun terakhir, kejahatan yang pelihatkan pembobolan atau pencurian informasi semakin gencar dan meyasar tidak hanya perorangan dan industri tetapi juga hingga ke level

[4] *Peta Jalan Strategi Nasional Pertahanan Siber*. Jakarta: Kementerian Pertahanan RI. 2014

[5] Peraturan Menteri Pertahanan No.82 tahun 2014, Pedoman Pertahanan Siber. Jakarta: Kementerian Pertahanan RI. Hal. 1

pemeritahan dalam bentuk penyadapan oleh intelijen luar negeri terhadap sejumlah pejabat pemerintahan Indonesia sehingga keamanan informasi sudah selayaknya mendapatkan prioritas khususnya dalam menunjang kebutuhan hankamnas.[6]

Saat ini bukan terjadi perang fisik, melainkan perang informasi dan data. Sejalan dengan itu, era teknologi informasi dan komunikasi membuat sebagian data telah dikemas dalam format digital. Untuk itu, permasalahan siber nasional menjadi salah satu isu strategis yang berpotensi mengancam keamanan siber di Indonesia. Seiring dengan banyaknya kasus yang mengancam keamanan informasi berbagai instansi pemerintah maupun swasta, maka pertahanan siber menjadi hal yang penting yang harus diperhatikan oleh setiap negara. Dahulu yang tadinya pertahanan siber hanya dianggap sebagai bagian dari bidang departemen teknologi informasi, kini *cyber security* merupakan tanggungjawab seluruh lembaga maupun instansi.

Sarana dan prasarana yang digunakan untuk menyimpan atau bertukar informasi harus dapat dijamin keamanannya dan harus dipastikan tidak ada celah kebocoran yang menyebabkan informasi strategis suatu organisasi atau pemerintahan dapat dengan mudah dicuri atau disadap. Oleh sebab itu, kebijakan terhadap bidang TIK sangat dibutuhkan terkait standarisasi keamanan perangkat sarana dan prasarana agar fungsi dan kegunaan yang dipakai di Indonesia dapat dipertanggungjawabkan untuk menjadi keamanan infomasi yang dipertukarkan melalui perangkat atau sarana prasarana tersebut. Semua hal ini dilakukan agar setiap kegiatan pertukaran informasi di Indonesia tetap terjamin validitas dan kerahasiaanya sehingga informasi yang dipertukarkan tetap terjamin validitas dan kerahasiaannya sehingga keakuratan informasi dapat dipertanggungjawabkan dan tidak menyesatkan pihak lain.[7]

Pemerintah selalu memiliki suatu kebijakan dalam menjalankan kepentingan untuk kemajuan bersama. Hal tersebut dijelaskan oleh Edi Suharto bahwa kebijakan merupakan sebuah

[6] Kiblat.mht, 2015; Richardus, Eko, & Indrajit, 2011 dalam Pradono, Wirianto. Yourdan. *Analisis Kebijakan Standarisasi Keamanan Perangkat Telekomunikasi Untuk Menunjang Kebijakan Pertahanan dan Keamanan Nasional.* Jakarta: Buletin Pos dan Telekomunikasi Vol 13 No.2 (2015) . Hal.151

[7] Paryati. Murya Y. 2008, Sistem Informasi. Yogyakarta : Ardana Media. Hal.379

instrument pemerintahan, bukan saja dalam arti government yang hanya menyangkut aparatur negara, melainkan pula government yang menyentuh pengelolaan sumber daya publik.[8] Oleh karena banyak hal yang melatarbelakangi urgensi pertahanan siber, pemerintah pun mengeluarkan berbagai kebijakan tentang pertahanan siber.

Kebijakan bidang TIK yang terkait standarisasi keamanan pernagkat telekomunikasi memiliki peranan penting agar fungsi dan kegunaan perangkat telekomunikasi yang beredar di Indonesia dapat dipertanggungjawabkan dan terutama untuk menjamin keamanan informasi yang dipertukarkan melalui perangkat tersebut. Pertahanan siber perlu dibangun sebagai suatu domain baru pertahanan sejalan dengan perkembangan teknologi dan dinamika geo-politik. Berikut merupakan kebijakan TIK dalam rangka Pertahanan Negara yang digunakan sebagai dasar pertahanan siber:

1. Undang-undang dasar No.11 Tahun 2008 tetang Informasi dan Transaksi Elektronik (UU ITE)[9]
2. Undang-Undang No. 3 Tahun 2002 tentang Pertahanan Negara[10]
3. Peraturan presiden No.97/2015 tentang Kebijakan Umum Pertahanan Negara Tahun 2015-2019 dengan pokok-pokok jakhaneg diantaranya pembangunan TIK pertahanan guna peningkatan kualitas Sisfohanneg[11]
4. Peraturan Pemerintah Penyelenggara Sistem dan Transaksi Elektronik (PP PSTE) No. 82/2012 semua itu merupakan pondasi membangun Keamanan Siber dan Pertahanan Siber Nasional.[12]
5. Perarturan Mentri Pertahanan No. 68 Tahun 2014 tentang Pengamanan Informasi di Lingkungan Kementerian Pertahanan dan Tentara Nasional Indonesia[13]
6. Perarturan Mentri Pertahanan No.82 Tahun 2014 tentang Pedoman Pertahanan Siber[14]

Kebijakan TIK pertahanan merupakan pembangunan TIK bidang Pertahanan yang diarahkan untuk

[8] Edi Suharto. 2011. Kebijakan Sosial Sebagai Kebijakan Publik. Bandung: Alfabeta. Hal.106

[9] Undang-undang dasar No.11 Tahun 2008 tetang Informasi dan Transaksi Elektronik

[10] Undang-Undang No. 3 Tahun 2002 tentang Pertahanan Negara

[11] Peraturan presiden No.97/2015 tentang Kebijakan Umum Pertahanan Negara Tahun 2015-2019

[12] Peraturan Pemerintah Penyelenggara Sistem dan Transaksi Elektronik (PP PSTE) No. 82/2012

[13] Perarturan Mentri Pertahanan No. 68 Tahun 2014 tentang Pengamanan Informasi di Lingkungan Kementerian Pertahanan dan Tentara Nasional Indonesia

[14] Perarturan Mentri Pertahanan No.82 Tahun 2014 tentang Pedoman Pertahanan Siber

meningkatkan kualitas Sisfohanneg termasuk Pertahanan Siber, yang dilakukan secara bertahap, berkesinambungan dan terintegrasi dalam pengelolaan Pertahanan Negara. Diperlukan organsasi yang memiliki sumber daya manusia yang kompeten danorganisasi TIK yang efektif, pembangunan proses TIK yang terarah, terukur dan terkelola dengan baik, dan pembangunan *enterprise architechture* yang terintegrasi.

Saat ini Kementerian Pertahanan Republik Indonesia sedang membangun Sistem Informasi Pertahanan Negara atau lebih dikenal lagi dengan istilah Sisfohanneg yang berbasis pada penyediaan data dan informasi yang cepat, akurat, real time sehingga aman dalam proses penetapan kebijakan keputusan. Keberadaan Sisfohanneg sangat penting sekali dimasa damai guna menghadapi perang informasi seperti saat ini prioritas pengembangan Sisfohanneg dibagi dalam 5 (lima) prioritas yakni (1) Sistem jaringan komunikasi data, (2) Sistem Aplikasi, (3) Up dating data secara online, (4) sistem keamanan data/sandi dan (5) pembinaan sumber daya manusia (SDM) bidang teknologi informasi dan komunikasi (TIK).[15]

Dalam Negara Undang - Undang Nomor 3 Tahun 2002 tentang Pertahanan menetapkan bahwa dalam sistem pertahanan negara terdiri dari ancaman militer dan ancaman non militer termasuk diantaranya adalah ancaman siber.[16] Oleh karena itu, sebagai upaya pencegahan terhadap serangan siber ini diperlukan sebuah lembaga yang bertugas menjadi benteng pertahanan dunia siber *(cyber defense).* Kementerian pertahanan mempunyai suatu organisasi khusus yang mengelola management basis data dan lalu lintas informasi yang terpusat, bernama Pusat Data dan Informasi Kementerian Pertahanan (Pusdatin Kemhan).

Pusdatin Kemhan adalah unsur pelaksana tugas yang melaksanakan pembinaan, pengembangan, dan standarisasi teknis serta evaluasi kebijakan di bidang sistem informasi dan persandian serta teknologi informasi di lingkungan kemhan. Didalam Pusdatin Kemhan, terdapat tim yang berkecimpung di dunia TIK meliputi

[15] Media Informasi Kementerian Pertahanan WIRA Vol.34 No.18. 2012. Jakarta: Kementerian Pertahanan RI. Hal.17

[16] Undang - Undang Nomor 3 Tahun 2002 tentang Pertahanan

bagian dari preventif (pencegahan), analisis bentuk ancaman, monitoring (pengawasan) terhadap ancaman atau gangguan dari pada *hecker, recovery* (Perbaikan/pembenahan), *attack* (Penyerangan) dan tim administrasi, yaitu *Cyber Operation Center (COC).*

Cyber Operation Centre dalam tataran kebijakan cyber security nasional pembentukannya ditujukan untuk membangun sistem pertahanan semesta yang melibatkan seluruh warga negara, wilayah dan sumber daya nasional lainnya untuk menegakkan kedaulatan negara, keutuhan wilayah dan keselamatan segenap bangsa dari ancaman *cyber*. Seiring berjalannya pelaksanaan keamanan siber di COC, terdapat beberapa permasalahan.

Pertama adalah dari komunikasi antar Kementerian/Lembaga (K/L) terkait. Belum optimalnya sinergitas antar K/L di seluruh Indonesia maupun sinergitas di lingkungan Kementerian Pertahanan Sendiri. Kedua, adalah dari sumberdaya, pemahaman para pegawai mengenai sadar bahwa menjaga aset strategis sangat penting, dan juga kurangnya sumber daya manusia bidang teknologi informasi. Ketiga adalah dari keamanan informasiya sendiri, dengan belum adanya payung hukum yang kuat untuk memayungi keamanan informasi di Indonesia. Menjadikan kemhan melakukan cara untuk melindungi aset strategisnya dari ancaman negara lain secara rahasia dengan lewat underground (bawah tanah). Kemhan memiliki 526 server yang tertanam dibawah tanah di tiap negara.[17]

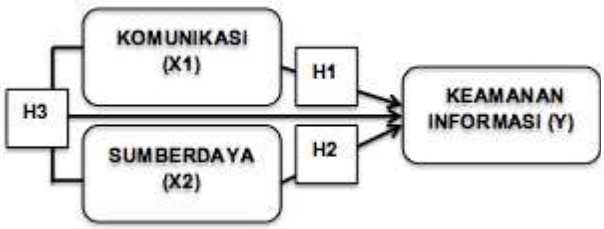
COC sebagai *embrio cyber defence* saat ini baru dilaksanakan sampai dengan tahap "siap operasional" padahal ancaman siber kini semakin marak berdasarkan laporan statistic yang sudah terpublikasi tetapi Pusdatin khususnya COC belum teridentifikasi upaya untuk meningkatkan keamanan informasi. Berdasarkan latar belakang masalah diatas, peneliti ingin melakukan penelitian lebih lanjut dengan judul Pengaruh Komunikasi dan Sumberdaya Terhadap Keamanan Informasi di Badan *Cyber Operation Center* Pusat Data dan Informasi Kementerian Pertahanan Republik Indonesia.

Dengan demikian bertujuan untuk menganalisa seberapa besar pengaruh komunikasi dan sumberdaya terhadap keamanan informasi di badan *cyber operation center* pusat data dan informasi kementerian pertahanan republic Indonesia. Dengan hipotesis:

[17] Kolonel Chb Dominggus Pakel, S.Sos, Kabid Dukops Pusdatin Kemhan RI, Juli 2017.

1. Terdapat pengaruh positif dan signifikan antara komunikasi dan keamanan informasi di badan *cyber operation center* pusdatin kemhan.
2. Terdapat pengaruh positif dan signifikan antara sumberdaya dan keamanan informasi di badan *cyber operation center* pusdatin kemhan.
3. Terdapat pengaruh positif dan signifikan Komunikasi dan Sumberdaya secara bersama-sama terhadap Keamanan Informasi di badan *cyber operation center* pusdatin kemhan.

Gambar 1.1 Skema Kerangka



Konseptual

Sumber: Data Primer Diolah, 2017

METODOLOGI

Pengumpulan data dalam penelitian ini dilakukan dengan cara menyebarkan kuesioner. Kuesioner itu sendiri adalah teknik pengumpulan data yang dilakukan dengan cara memberi serangkaian pertanyaan atau pernyataan tertulis kepada responden untuk mendapatkan data yang relevan mengenai variabel yang diteliti. [18]

Populasi yang akan diteliti adlaah populasi para pelaksana kebijakan pertahanan siber Pusdatin Kemhan total berjumlah 140 orang dari 4 sub bagian. Sampel adalah bagian dari jumlah dan karateristik yang dimiliki oleh populasi tersebut. Populasi pada Badan Cyber Operation Center Pusdatin Kementerian Pertahanan total berjumlah 140 orang. Teknik pengambilan sampel menggunakan metode random sampling, kemudian penentuan besarnya sampel menggunakan rumus Slovin sebagai berikut:

Rumus Slovin tersebut adalah:

$$n = \frac{N}{1 + N\,(e)^2} \qquad (3.1)$$

dimana:

n = Jumlah Sampel

N = Jumlah Populasi

E2 = Taraf Kesalahan 5%

Sehingga berdasarkan rumus tersebut diperoleh jumlah sampel sebagai berikut:

$$n = \frac{140}{1 + 140(0{,}05)^2} = 103{,}703$$

atau dengan kata lain 130 responden sudah memenuhi batas

[18] Sugiyono. (2013). Metode Penelitian Kuantitatif Kualitatif dan R&D. Bandung : Alfabeta. Hal.41.

minimal yang dibutuhkan. Dibulatkan menjadi 103 yang dijadikan sebagai sampel penelitian sesuai jumlah populasi pelaksana kebijakan pertahanan siber Pusdatin Kemhan.

Uji instrument menggunakan uji validitas dan reliabilitas. Uji validitas dengan dasar pengambilan keputusan sebagai berikut:

a. Jika coefficient correlation ≥ 0,5 maka item pernyataan valid
b. Jika coefficient correlation < 0,5 maka item pertanyaan tidak valid

Uji reliabilitas dengan dasar pengambilan keputusan sebagai berikut:

a. Jika cronbach's alpha $\geq 0{,}6 \rightarrow$ cronbach's alpha reliable (construct reliable).
b. Jika cronbach's alpha $< 0{,}6 \rightarrow$ cronbach's alpha poor reliable (construct unreliable).

Uji asumsi klasik terdiri dari uji normalitas, uji multikolinieritas, uji autokorelasi, dan uji heterokedastisitas. Berikut dasar pengambilan keputusan uji normalitas:

a. Jika sig. ≥ 0,05 maka data terdistribusi normal dan asumsi normalitas terpenuhi.
b. Jika sig. < 0,05 maka data tidak terdistribusi normal dan asumsi normalitas tidak terpenuhi.

Uji multikolinieritas dengan dasar pengambilan keputusan sebagai berikut:

a. Jika VIF > 10 ada Multikolinearitas.
b. JIka VIF < 10 tidak ada Multikolinearitas.

Uji autokorelasi dengan dasar pengambilan keputusan sebagai berikut:

a. Jika d lebih kecil dari dL atau lebih besar dari (4-dL) maka hipotesis nol ditolak, yang berarti terdapat autokorelasi.
b. Jika d terletak antara dU dan (4-dU), maka hipotesis nol diterima, yang berarti tidak ada autokorelasi.
c. Jika d terletak antara dL dan dU atau diantara (4-dU) dan (4-dL), maka tidak menghasilkan kesimpulan yang pasti.

Uji heterokedasitas dengan dasar pengambilan keputusan sebagai berikut:

a. Jika Sig dari t < 0.05 maka Ho ditolak (ada heterokedastisitas).
b. Jika Sig dari t > 0.05 maka Ho diterima (tidak heterokedastisitas).

Metode analisis data dalam penelitian ini menggunakan multiple regresion (regresi berganda). Pengujian hipotesa dilakukan dengan cara membandingkan p-value dari hasil analisa setiap hipotesa dalam penelitian ini dengan level of significant (α) sebesar 0.05 dan pengambilan keputusan

berdasarkan:

a. Jika p-value ≤ 0,05 : signifikan secara statistik, maka H0 ditolak.
b. Jika p-value > 0,05 : tidak signifikan secara statistik, maka H0 diterima.

Uji hipotesis terdiri dari uji t, uji F dan uji koefisien determinasi. Berikut dasar pengambilan keputusan uji t:

a. Jika t Hitung < t Tabel, maka H0 diterima.
b. Jika t Hitung > t Tabel, maka H0 ditolak.

Uji F dengan dasar pengambilan keputusan sebagai berikut:

a. Jika nilai F hitung > F tabel maka variabel bebas (X) berpengaruh terhadap variabel terikat (Y).
b. Jika nilai F hitung < F tabel maka variabel bebas (X) tidak berpengaruh terhadap variabel terikat (Y).

Uji koefisien determinasi dengan dasar pengambilan keputusan sebagai berikut:

a. Nilai R^2 yang kecil berarti kemampuan variabel-variabel independen dalam menjelaskan variasi-variabel dependen sangat terbatas, sebaliknya
b. Nilai R^2 yang mendekati satu berarti variabel independen memberikan hampir semua informasi yang dibutuhkan untuk memprediksi variasi dependen.

PEMBAHASAN

Statistik Deskriptif

Deskriptif karateristik responden dalam penelitian ini dijelaskan menjadi dua bagian. Bagian tersebut melipti pengelompokan berdasarkan usia, pendidikan dan lama bekerja. Berdasarkan usia maka responden dibagi menjadi 4 kelompok umur, yaitu 24-30 tahun, 31-43 tahun, 38-43 tahun, dan 44-50 tahun. Dari hasil kuesioner terhadap 103 orang responden, memperlihatkan bahwa responden berusia 24-30 tahun sebanyak 12 orang atau 11,6%, 38-42 sebanyak 9 orang atau 8,7%, dan 44-50 sebanyak 5 orang atau 4,9%.

Dalam penelitian ini, pengelompokkan responden juga dilakukan berdasarkan tingkat pendidikan. Kategori responden berdasarkan tingkat pendidikan memperlihatkan bahwa responden dengan tingkat pendidikan SMU sebanyak 1 orang atau 0,9%, kemudian dengan tingkat pendidikan D3 sebanyak 4 orang atau 4%, lulusan S1 sebanyak 91 orang atau 88,3%, dan tingkat pendidikan S2 sebanyak 7 orang atau 6,8%.

Selanjutnya peneliti melakukan skoring kriteria penilaian untuk variabel

Keamanan Informasi (Y). Diketahui bahwa prosentase jawaban responden paling tinggi terhadap variabel Keamanan Informasi (Y), responden menyatakan setuju dengan skor 1115 kali atau 54,12%. Hal ini menunjukkan bahwa tanggapan responden untuk variabel Keamanan Informasi (Y) mendapat skor sebesar 54,12% yang mempunyai kriteria yang baik. Sehingga dapat disimpulkan bahwa Keamanan Informasi pada badan cyber operation center Pusdatin Kemhan RI memiliki komunikasi yang baik antar pembuat kebijakan dengan pelaksana kebijakan. Pelaksana atau badan cyber dapat menerima seluruh materi mengenai SOP keamanan informasi terbaru dengan baik pula demi terjaganya informasi strategis Kementerian Pertahanan Republik Indonesia.

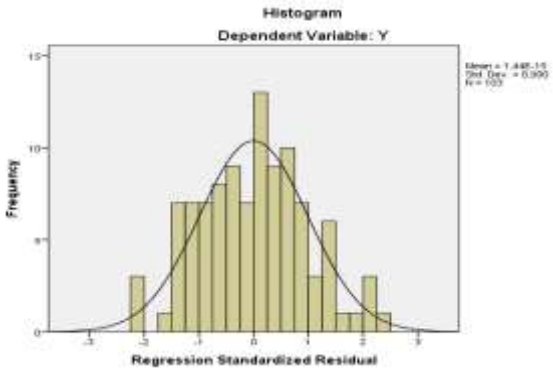
Berdasarkan hasil tanggapan responden terhadap variabel Komunikasi (X1) dapat diketahui bahwa prosentase jawaban responden paling tinggi terhadap variabel Komunikasi (X1), responden menyatakan setuju dengan skor 1208 kali atau 58,64%. Hal ini menunjukkan bahwa tanggapan responden untuk variabel Komunikasi (X1) mendapat skor sebesar 58,64% yang mempunyai kriteria yang baik. Sehingga dapat disimpulkan Keamanan Informasi pada badan cyber operation center Pusdatin Kemhan RI memiliki komunikasi yang tinggi. Para personel Pusdatin beranggapan bahwa komunikasi yang terjalin antar regulator dan implementor berjalan dengan baik.

Berdasarkan hasil data tanggapan responden terhadap variabel Sumberdaya (X2) dapat diketahui bahwa prosentase jawaban responden paling tinggi terhadap variabel Sumberdaya (X2), responden menyatakan setuju dengan skor 1281 kali atau 62,18%. Hal ini menunjukkan bahwa tanggapan responden untuk variabel Sumberdaya (X2) mendapat skor sebesar 62,18% yang mempunyai kriteria yang baik. Sehingga dapat disimpulkan Keamanan Informasi pada badan cyber operation center Pusdatin Kemhan RI memiliki sumberdaya manusia, sarana prasana yang baik. Para personel Pusdatin beranggapan bahwa Sumberdaya yang ada di Pusdatin Kemhan RI sudah cukup lengkap dan selalu uptodate sehingga dapat bertugas menjalankan tupoksi dengan baik.

Uji Asumsi Klasik

Hasil uji normalitas didapatkan nilai asymptotic significance lebih besar dari α 0.05 sehingga dapat dikatakan bahwa

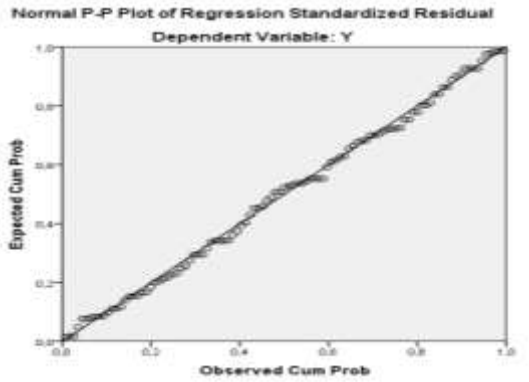
data yang digunakan adalah normal.



Gambar 3.1 Grafik Normalitas

Sumber: Data Primer Diolah, 2017

Pada grafik histogram normalitas diatas, terlihat residual terdistribusi secara normal dan simetris tidak menceng kiri atau kanan. Sehingga model ini dapat dikatakan berdistribusi normal.

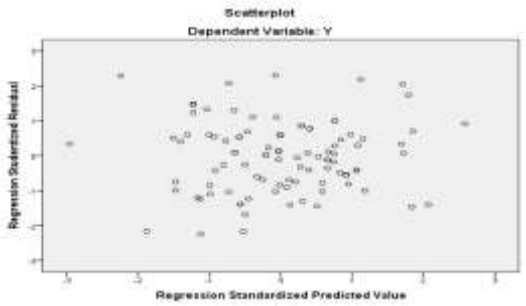


Gambar 3.2 Grafik Normal Plot Normalitas

Sumber: Data Primer Diolah, 2017

Pada grafik normal p-plot diatas, terlihat model regresi memenuhi asumsi normalitas karena data menyebar di sekitar garis diagonal dan mengikuti arah garis diagonal.

Hasil uji heterokedasitas menjelaskan pada gambar 3.3 tidak ada pola yang jelas, serta titik-titik menyebar di atas dan di bawah angka 0 pada sumbu Y, maka tidak terjadi heterokedasitas pada model regresi.



Gambar 3.3 Grafik Heterokedastisitas

Sumber: Data Primer Diolah, 2017

Hasil pengujian multikolinearitas, hasil perhitungan nilai tolerance tidak ada variabel independen yang memiliki nilai tolerance < 0,10 yang artinya tidak ada korelasi antara variabel independen yang lebih dari 95%. Demikian juga dengan hasil perhitungan nilai VIF, dari kedua variabel independen yang diuji tidak ada nilai VIF yang lebih besar dari 10, maka dapat disimpulkan bahwa tidak ada multikolinieritas antara variabel independent dalam model regresi.

Hasil uji multikolinearitas didapatkan nilai: a) variabel Komunikasi tidak terdapat multikolinearitas, karena besarnya nilai VIF (*Variance Inflation Factor*) lebih kecil dari 10, atau 1,453 < 10 dengan *tolerance* 0,688; b) Untuk variabel Sumberdaya tidak terdapat multikolinearitas, karena besarnya nilai VIF (*Variance Inflation Factor)* lebih kecil dari 10, atau 1,453 < 10 dengan *tolerance* 0,688.

Hasil uji autokorelasi, diketahui model regresi yang digunakan berada pada daerah tidak ada autokorelasi (positif atau negatif) Ho diterima. Berdasarkan hasil uji Durbin-Watson menunjukkan nilai DW sebesar 1,872. Nilai ini kemudian dibandingkan dengan nilai tabel menggunakan derajat kepercayaan 5% jumlah sampel 103 dan jumlah variabel bebas 2 (k=2). Dari tabel Durbin-Watson didapatkan nilai dl = 1,6396 dan du = 1,7186 Setelah dolakukan pemetaan, nilai DW 1,872 Terletak antara batas atas (du) yaitu 1,7186 (4-du) yaitu 2,128, maka dapat disimpulkan tidak terdapat autokorelasi pada model regresi tersebut du < dW < 4-dU ; 1,7186 < 1,1872 < 2,128. DW berada diantara dU dan 4-dU sehingga dapat dikatakan tidak ada autokorelasi baik (+) maupun (-).

Uji Hipotesis

Tabel 3.1 Hasil Uji t

Model	Standardized Coefficients	t	Sig.
	Beta		
(Constant)		8,256	,000
Komunikasi	,362	3,694	,000
Sumberdaya	,298	3,041	,003

Sumber: Data Primer Diolah, 2017

Hipotesis 1 : Terdapat pengaruh yang positif dan signifikan antara Komunikasi (X1) terhadap Keamanan Informasi (Y)

Komunikasi memiliki peran yang sangat penting dalam sebuah implementasi kebijakan. Keberhasilan implementasi kebijakan mensyaratkan agar implementor mengetahui apa yang harus dilakukan.[19] Artinya adalah untuk mencapai sebuah keberhasilan implementasi kebijakan harus ada komunikasi yang baik dari pembuat kebijakan terhadap pelaksana kebijakan agar pelaksana kebijakan juga dapat mentransmisikan kepada kelompok sasaran (target group) apa yang menjadi tujuan kebijakan.

Komunikasi antara implementor dengan target sasaran untuk mewujudkan Keamanan Informasi yang baik di Pusat Data dan Informasi Kementerian Pertahanan Republik Indonesia dilakukan dengan cara sosialisasi tentang pentingnya pertahanan siber dari aparat pelaksana kepada sumberdaya manusia dan stakeholder terkait. Sosialisasi berupa pelatihan keterampilan pertahanan siber pada kelompok sasaran.

Hasil uji t untuk X1 diperoleh t hitung = 3.694 dengan tingkat signifikansi sebesar 0,000. Dengan menggunakan batas signifikansi 0,05 dan df (n-2) yakni

[19] Edward III dalam Subarsono (2005) Analisis Kebijakan Publik (Konsep, Teori dan Aplikasi). . Hal. 90

101 didapat t tabel sebesar 1,663. Berdasarkan data diatas didapatkan hasil bahwa t hitung (3.694) lebih besar t tabel (1.663), yang berarti H0 ditolak dan H1 diterima. Hal ini menunjukkan bahwa ada pengaruh yang sgnifikan antara Komunikasi (X1) terhadap Keamanan Informasi (Y). Berdasarkan hasil perhitungan uji regresi linier berganda untuk variabel Komunikasi diperoleh sebesar 26,2 %.

Dalam penelitian ini bedasarkan perhitungan statistik dapat diketahui bahwa komunikasi dalam implementasi kebijakan pertahanan siber, keamanan informasi pada Pusat Data dan Informasi Kementerian Pertahanan Republik Indonesia masuk kedalam kategori baik. Berdasarkan hasil perhitungan uji regresi linier berganda untuk variabel Komunikasi diperoleh sebesar 26,2%. Nilai koefisien regresi bertanda positif menunjukkan bahwa kontribusi variabel Komunikasi (X1) terhadap Keamanan Informasi (Y) adalah positif, yang artinya setiap terjadi kenaikan satu unit skor variabel Komunikasi (X1) maka akan diikuti dengan meningkatnya Keamanan Informasi (Y) sebesar 0,262 pada konstanta 45,859. Berdasarkan hasil analisis uji t diperoleh t hitung 3,694 > t tabel 1,663, yang berarti hipotesis yang menyatakan ada pengaruh variabel Komunikasi (X1) terhadap Keamanan Informasi (Y) dapat diterima, dengan kata lain Keamanan Informasi tidak lepas dari adanya variabel Komunikasi.

Sehingga uji hipotesis pertama pada penelitian ini menunjukkan bahwa Komunikasi (X1) berpengaruh positif dan signifikan terhadap Keamanan Informasi (Y) dengan pengaruh yang diberikan oleh komunikasi terhadap keamanan informasi sebesar 26,2 persen. Artinya bahwa semakin baik Komunikasi yang tersedia maka semakin tinggi keberhasilan implementasi pertahanan siber keamanan informasi Pusdatin Kemhan RI dan berlaku sebaliknya jika semakin buruk implementasi pertahanan siber keamanan informasi Pusdatin Kemhan RI maka semakin rendah komunikasinya.

Hipotesis 2 : Terdapat pengaruh yang positif dan signifikan antara Sumberdaya (X1) terhadap Keamanan Informasi (Y)

Kebijakan publik adalah kebijakan yang kompleks dan menyangkut impak yang luas. [20]Oleh karena itu, implementasi kebijakan publik akan melibatkan berbagai sumberdaya yang diperlukan. Van Meter dan Van Horn (Winarno

[20] Hogwood dan Gunn dalam Nugroho, Riant. (2011). Analisis Kebijakan. Jakarta: PT Elex Media Komputindo. Hal.30

2088:158) menambahkan, disamping ukuran-ukuran dasar dan tujuan-tujuan kebijakan, yang perlu mendapat perhatian dalam proses implementasi adalah sumber daya yang tersedia.

Sumber daya merupakan hal yang penting dalam implementasi kebijakan pertahanan siber, baik itu sumber daya manusia maupun sarana dan prasarana. Ketersediaan sumber daya manusia yang memiliki kemampuan mengoperasikan software pengamanan dengan baik dan mampu memberikan gagasan atau ide baru yang konstuktif yang menjai salah satu kriteria pelaksana untuk menunjang keberhasilan implementasi pertahanan siber itu sendiri untuk menjaga keamanan informasi. Selain itu, sarana dan prasana pun penting untuk pelaksanaan pertahanan siber yang terdiri dari software, hardware, dan juga jaringan internet infranet dalam menjaga keamanan informasi.

Hasil uji t untuk X2 diperoleh thitung = 3,041 dengan tingkat signifikansi sebesar 0,003. Dengan menggunakan batas signifikansi 0,05 dan df (n-2) yakni 101 didapat t tabel sebesar 1,663. Berdasarkan data diatas didapatkan hasil bahwa t hitung (3.041) lebih besar t tabel (1.663), yang berarti H0 ditolak dan H2 diterima..Hal ini menunjukkan bahwa ada pengaruh yang sgnifikan antara Sumberdaya (X2) terhadap Keamanan Informasi (Y). Berdasarkan hasil perhitungan uji regresi linier berganda untuk variabel Komunikasi diperoleh sebesar 22,6 %.

Dalam penelitian ini bedasarkan perhitungan statistik dapat diketahui bahwa Sumberdaya dalam implementasi kebijakan pertahanan siber, keamanan informasi pada Pusat Data dan Informasi Kementerian Pertahanan Republik Indonesia masuk kedalam kategori baik. Berdasarkan hasil perhitungan uji regresi linier berganda untuk variabel Sumberdaya diperoleh sebesar 0,220. Nilai koefisien regresi bertanda positif menunjukkan bahwa kontribusi variabel Sumberdaya (X2) terhadap Keamanan Informasi (Y) adalah positif, yang artinya setiap terjadi kenaikan satu unit skor variabel Sumberdaya (X2) maka akan diikuti dengan meningkatnya Keamanan Informasi (Y) sebesar 0,220 pada konstanta 5,555. Berdasarkan hasil analisis uji t diperoleh t hitung 3,041 > t tabel 1,663, yang berarti hipotesis yang menyatakan ada pengaruh variabel Sumberdaya (X2) terhadap Keamanan Informasi (Y) dapat diterima, dengan kata lain Keamanan Informasi tidak lepas dari adanya variabel Sumberdaya.

Sehingga uji hipotesis pertama pada penelitian ini menunjukkan bahwa Sumber Daya (X2) berpengaruh positif dan signifikan terhadap Keamanan Informasi (Y) dengan pengaruh yang diberikan oleh sumberdaya terhadap keamanan informasi sebesar 22,6 persen. Artinya bahwa semakin baik sumber daya yang tersedia maka semakin tinggi keberhasilan implementasi pertahanan siber keamanan informasi Pusdatin Kemhan RI dan berlaku sebaliknya jika semakin buruk implementasi pertahanan siber keamanan informasi Pusdatin Kemhan RI maka semakin rendah sumber dayanya.

Hipotesis 3: Variabel Komunikasi (X1), Sumberdaya (X2) secara serentak atau bersama-sama berpengaruh positif dan signifikan terhadap variabel terikat Keamanan Informasi (Y)

Tabel 3.2 Hasil Uji F

Model		F	Sig.
1	Regression	25,747	.000[b]
	Residual		
	Total		

Sumber: Data Primer Diolah, 2017

Nilai F tabel dapat dilihat pada tabel F dengan tingkat signifikansi 0,05 dengan df 1 (jumlah variabel-1) = 3–1 = 2,d an df 2 (n-k-1) atau 103-3-1 = 99 (n adalah jumlah data dan k adalah jumlah variabel bebas). Karena nilai F hitung (25.747) . F tabel 3,08 dan nilai signifikansi dibawah 0,05 maka H0 ditolak dan H1 diterima. Maka dapat disimpulkan H1 diterima dan H0 ditolak yang artinya variabel Komunikasi (X1) dan Sumberdaya (X2) secara simultan atau bersama – sama mempengaruhi variabel Keamanan Informasi (Y).

Tabel 3.3 Hasil Koefisien Determinasi

R	Adjusted R Square
.583[a]	.347

Sumber: Data Primer Diolah, 2017

Dari tabel 4.15 diatas diketahui bahwa besarnya nilai adjusted R2 sebesar 0,327 yang mempunyai arti bahwa variasi Keamanan Informasi (Y) dapat dijelaskan oleh variasi ketiga variabel independen yaitu Komunikasi (X1) dan Sumberdaya (X2) sebesar 32.7%, sedangkan sisanya dijelaskan oleh faktor lain diluar model.

Dengan demikian bukan hanya Komunikasi dan Sumberdaya yang dapat mempengaruhi Keamanan Informasi di Pusdatin Kemhan tetapi ada variabel lain yang ikut berperan dalam meningkatkan Keamanan Informasi pada Pusdatin Kemhan RI. Hal ini memberikan peluang bagi peneliti lain yang ingin melakukan penelitian selanjutnya terkait dengan Keamanan Informasi di Pusdatin Kemhan RI.

Berdasarkan hasil regresi ordinal juga dapat diketahui bahwa untuk semua Variabel Komunikasi, Sumberdaya, secara bersama-sama memberikan pengaruh pada implementasi pertahanan siber keamanan informasi Pusdatin Kemhan RI. Sehingga hipotesis ketiga dalam penelitian ini menunjukkan bahwa komunikasi dan sumberdaya secara bersama-sama berpengaruh positif dan signifikan terhadap implementasi pertahanan siber keamanan informasi Pusdatin Kemhan RI. Berdasarkan hasil penelitian dan pembahasan maka telah membuktikan bahwa teori George C. Edward III (1980) [21] yang menyatakan komunikasi dan sumberdaya, memang memiliki pengaruh terhadap implementasi kebijakan pertahanan siber keamanan informasi di Badan Cyber Operation Center Pusat Data dan Informasi Kementerian Pertahanan Republik Indonesia.

SIMPULAN

Berdasarkan hasil penelitian, dapat ditarik kesimpulan bahwa komunikasi dan sumberdaya berpengaruh positif terhadap Keamanan Informasi Badan Cyber Operation Center Kementerian Pertahanan Republik Infonesia, berikut penjelasannya:

a. Terdapat pengaruh positif Komunikasi terhadap Keamanan Informasi Badan Cyber Operation Center Kementerian Pertahanan Republik Infonesia dengan pengaruh signifikan sebesar 26,2%. Hal tersebut menunjukan bahwa semakin baik Komunikasi maka semakin baik Keamanan Informasi.
b. Terdapat pengaruh positif Sumberdaya terhadap Keamanan Informasi Badan Cyber Operation Center Kementerian Pertahanan Republik Infonesia dengan pengaruh signifikan sebesar 22,6%. Hal tersebut menunjukan bahwa semakin baik Sumberdaya maka semakin baik Keamanan Informasi.
c. Terdapat pengaruh positif Komunikasi dan Sumberdaya terhadap Keamanan Informasi Badan Cyber Operation Center Kementerian Pertahanan Republik Infonesia dengan pengaruh signifikan sebesar 32,7 %. Hal tersebut menunjukan bahwa semakin baik Komunikasi dan Sumberdaya maka semakin tinggi Keamanan Informasi.

[21] George C. Edward III dalam Subarsono (2011) Analisis Kebijakan Publik (Konsep, Teori dan Aplikasi). Hal.90

SARAN

Berdasarkan hasil penelitian dan simpulan, peneliti mengajukan saran-saran dengan harapan dapat bermanfaat bagi semua pihak yang berkepentingan. Adapun saran-saran yang akan peneliti kemukakan sebagai berikut:

Saran Teoritis

a. Perlu penelitian lebih lanjut mengenai variabel lainnya yang mempengaruhi implementasi kebijakan pertahanan siber misalnya variabel disposisi dan struktur birokrasi
b. Perlu penelitian lebih lanjut mengenai sinergitas antar badan di kementerian pertahanan dalam pemeliharaan sistem informasi pertahanan negara, atau sinergitas antar K/L di Indonesia dalam menjaga keamanan informasi strategis.

Saran Praktis

1. Variabel Keamanan Informasi
   a. Berdasarkan hasil penelitian, indikator terendah yang berkaitan dengan keamanan informasi adalah informasi atau data akan selalu tersedia saat dibutuhkan. Hal ini perlu menjadi evaluasi bagi Kementerian Pertahanan untuk melakukan upaya agar para pelaksana kebijakan pertahanan siber dapat menerima informasi dan data dengan lengkap dan selalu tersedia apablika dibutuhkan sesuai dengan SOP yang berlaku
   b. Berdasarkan hasil penelitian, indikator tertinggi yang berkaitan dengan keamanan informasi adalah data yang dikirim, diterima dan disimpan bersifat rahasia. Hal ini perlu menjadi evaluasi bagi Kementerian Pertahanan untuk dapat mempertahankan bahkan meningkatkan keamanan informasi pada kerahasiaan informasi strategis pertahanan dengan SOP yang berlaku.
2. Variabel Komunikasi
   a. Berdasarkan hasil penelitian, indikator terendah yang berkaitan dengan komunikasi adalah informasi yang diberikan tidak berubah-ubah (konsisten). Hal ini perlu menjadi evaluasi bagi Kementerian Pertahanan agar dalam memberikan informasi mengenai pertahanan siber senantiasa terus konsisten dan tidak berubah sehingga menjadikan para pelaksana kebijakan pertahanan siber dapat bekerja dengan fokus dalam menjaga keamanan informasi tanpa dinamika perubahan informasi yang tidak konsisten.

b. Berdasarkan hasil penelitian, indikator tertinggi yang berkaita dengan komunikasi adalah Koordinasi pelaporan kegiatan setiap bulan (evaluasi kegiatan tiap bulan). Hal ini pelu menjadi evaluasi bagi Kementerian Pertahanan untuk dapat mempertahankan bahkan meningkatkan kualitas evaluasi kegiatan agar keamanan informasi selalu terjaga kerahasiaannya dan seluruh kegiatan berjalan dengan lebih baik.

3. Variabel Sumberdaya

a. Berdasarkan hasil penelitian, indikator terendah yang berkaitan dengan sumberdaya adalah alokasi dana tepat sasaran. Hal ini perlu menjadi evaluasi bagi Kementerian Pertahanan agar senantiasa membuat rencana belanja untuk pengamanan informasi strategis pertahanan dengan baik dan tepat sasaran agar bisa dipergunakan untuk terus memperbaharui sumberdaya pertahanan (manusia, sarana dan prasarana).

b. Berdasarkan hasil penelitian, indikator tertinggi yang berkaitan dengan sumberdaya adalah peralatan penunjang hardware maupun software pendukung selalu diperbaharui sesuai dengan prosedur yang ada. Hal ini perlu menjadi evaluasi bagi Kementerian Pertahanan untuk dapat mempertahanankan bahkan meningkatkan pembaharuan yang terus menerus dengan mengikuti perkembangan teknologi agar keamanan informasi strategis pertahanan negara terjaga lebih kuat.

REFERENSI

Buku

Edwards, George C. (1980). *Implementing Pubic Policy. USA: Library of Congress Cataloging in Publication Data*

Nugroho, Riant. (2011). Analisis Kebijakan. Jakarta: PT Elex Media Komputindo

Paryati, Murya Y. (2008). Sistem Informasi. Yogyakarta: Ardana Media.

Richardus, Eko, & Indrajit. (2011). Manajemen Keamanan Informasi Dan Internet. Jakarta: Kementerian Komunikasi dan Informatika RI

Subarsono, AG. (2005). Analisis Kebijakan Publik (Konsep, Teori dan Aplikasi). Yogyakarta: Pustaka Pelajar

Sugiyono. (2013). Metode Penelitian Kuantitatif Kualitatif dan R&D. Bandung: Alfabeta

Suharto, Edi. (2011). Kebijakan Sosial Sebagai Kebijakan Publik. Bandung: Alfabeta

Dokumen dan Peraturan

Undang-undang dasar No.11 Tahun 2008 tetang Informasi dan Transaksi Elektronik (UU ITE)

Undang-Undang No. 3 Tahun 2002 tentang Pertahanan Negara

Perpres No.97/2015 tentang Kebijakan Umum Pertahanan Negara Tahun 215-2019

Peraturan Pemerintah Penyelenggara Sistem dan Transaksi Elektronik (PP PSTE) No. 82/2012

Peraturan Kementerian Pertahanan No.82 Tahun 2014 tentang Pedoman Pertahanan Siber

Kementerian Pertahanan RI. Peta Jalan Strategi Nasional Pertahanan Siber, Jakarta, 2014.

Jurnal dan Artikel

Pradono, Wirianto. Yourdan. Analisis Kebijakan Standarisasi Keamanan Perangkat Telekomunikasi Untuk Menunjang Kebijakan Pertahanan dan Keamanan Nasional. Jakarta: Buletin Pos dan Telekomunikasi Vol 13 No.2 (2015)

Media Informasi Kementerian Pertahanan WIRA Vol.34 No.18 Januari-Februari 2012

Sumber Lain

Website Kementerian Pertahanan RI www.kemhan.go.id diakses pada 28 Juli 2017

Website Pusat Data dan Informasi Kementerian Pertahanan RI www.pusdatin.kemhan.go.id diakses pada 28 Juli 2017