Analisis kebijakan standardisasi keamanan perangkat telekomunikasi untuk menunjang kebijakan pertahanan dan keamanan nasional

Policy analysis on telecommunication devices security standardization to support national security and defence policy

Wirianto Pradono[1], Yourdan[2]
[1,2]*Pusat Penelitian dan Pengembangan Sumber Daya dan Perangkat Pos dan Informatika*
[1,2]*Jl. Medan Merdeka Barat No.9 Jakarta 10110, Indonesia*
e-mail: [1]wiri001@kominfo.go.id, [2]yourd@kominfo.go.id

INFORMASI ARTIKEL

Naskah diterima 14 Desember 2015
Direvisi 22 Desember 2015
Disetujui 23 Desember 2015

Keywords:
Telecommunication
Devices standardization
Policy

ABSTRACT

In the past years, incidents involving information security breach increase significantly and cause huge damage to industry, government or individual. Due to that, information security needs to be well guaranteed especially when it comes to sensitive and confidential information. One has to be done to cope with that is the availibility of policy on telecommunication devices security standardization to assure validity and confidentiality of all information going through the devices. Both qualitative and quantitative method used in this study to describe implementation of telecommnunication devices security that has been done by both government and ICT industry and also to identify obstacles in implementation of telecommunication device security assurance for both public and special purposes, from technology, institutional, and regulation aspects. This study showed that any regulation related with telecommunication device security standardization for special purposes has not been provided yet. Besides, authorized institution to examine and certify telecommunication devices security especially for specific purposes has not been assigned yet.

Kata kunci :
Telekomunikasi
Standarisasi perangkat
Kebijakan

ABSTRAK

Beberapa tahun terakhir, kejadian yang terkait dengan pembobolan informasi meningkat dengan signifikan dan menyebabkan kerugian yang tidak sedikit baik bagi pemerintah, industri maupun perorangan. Oleh karenanya diperlukan jaminan terhadap keamanan informasi terutama yang menyangkut informasi yang sensitif dan rahasia. Untuk mengatasi hal tersebut, diperlukan kebijakan di bidang standarisasi keamanan perangkat telekomunikasi untuk menjamin validitas dan kerahasiaan informasi yang dilewatkan melalui perangkat tersebut. Pendekatan kualitatif maupun kuantitatif digunakan dalam studi ini untuk memperoleh gambaran tentang kondisi penerapan standar keamanan perangkat baik oleh pemerintah maupun industri telekomunikasi serta mengidentifikasi kendala yang dihadapi dalam menjamin keamanan perangkat telekomunikasi baik untuk kebutuhan umum maupun kebutuhan khusus baik dari aspek teknologi, kelembagaan, maupun regulasi. Hasil penelitian menunjukkan belum ada regulasi yang mengatur standarisasi keamanan perangkat telekomunikasi untuk kebutuhan khusus. Selain itu belum ada penetapan secara eksplisit tentang lembaga yang berwenang dalam pengujian dan sertifikasi keamanan perangkat telekomunikasi terutama untuk kebutuhan khusus. Sejumlah regulasi yang mengatur secara spesifik bidang standarisasi keamanan perangkat telekomunikasi saat ini masih dalam proses penyusunan oleh instansi-instansi terkait.

1. Pendahuluan

Pemanfaatan teknologi informasi dan komunikasi menyentuh hampir semua bidang mulai dari ekonomi, pendidikan, kesehatan hingga pertahanan dan keamanan. Teknologi informasi dan komunikasi sebagai salah satu unsur strategis dalam mendukung penyelenggaraan pertahanan dan keamanan sudah selayaknya mendapatkan perhatian lebih. Terlebih lagi dalam beberapa tahun terakhir, kejahatan yang melibatkan pembobolan atau pencurian informasi semakin gencar dan menyasar tidak hanya perorangan

dan industri tetapi juga hingga ke level pemerintahan dalam bentuk penyadapan oleh intelijen luar negeri terhadap sejumlah pejabat pemerintahan Indonesia sehingga keamanan informasi sudah selayaknya mendapatkan prioritas khususnya dalam menunjang kebutuhan hankamnas (Kiblat.mht, 2015; Richardus, Eko, & Indrajit, 2011). Perangkat telekomunikasi yang digunakan untuk bertukar informasi harus dapat dijamin keamanannnya dan tidak ada celah kebocoran yang menyebabkan informasi dapat dicuri atau disadap. Oleh karena itu, dibutuhkan kebijakan bidang TIK yang terkait standarisasi keamanan perangkat telekomunikasi agar fungsi dan kegunaan perangkat telekomunikasi yang beredar di Indonesia dapat dipertanggungjawabkan dan terutama untuk menjamin keamanan informasi yang dipertukarkan melalui perangkat tersebut. Hal ini dilakukan agar informasi yang dipertukarkan tetap terjamin validitas dan kerahasiaannya sehingga keakuratan informasi dapat dipertanggungjawabkan dan tidak menyesatkan pihak lain (Paryati, 2008). Selain itu untuk menjamin keamanan tersebut perlu melibatkan sejumlah *stakeholders* terkait baik pemerintah maupun industri (Wamala, 2011). Selain diperlukan kebijakan dan peran para stakeholders, hal lain yang juga perlu diperhatikan adalah keberadaan teknologi pengamanan yang memadai seperti misalnya aplikasi untuk menghapus informasi berharga dari *smartpohone* untuk mencegah data dicuri saat *smartphone* hilang (Wicaksono, 2007). Dalam kaitannya dengan kebutuhan akan kebijakan tersebut, kajian ini dilakukan untuk memperoleh gambaran awal yakni upaya penerapan keamanan perangkat telekomunikasi saat ini dan potensi serta kendala yang dihadapi dalam upaya penjaminan keamanan perangkat telekomunikasi baik untuk kebutuhan umum yakni masyarakat dan industri maupun kebutuhan khusus yakni militer, kepolisian, dan pejabat negara baik dari aspek teknologi, kelembagaan, maupun regulasi yang dirangkum ke dalam sejumlah pertanyaan penelitian yang dirumuskan berdasarkan perkembangan permasalahan pembobolan keamanan informasi yang diperoleh dari berbagai literatur baik buku maupun jurnal. Hasil penelitian yang diperoleh melalui metode kualitatif maupun kuantitatif ini dapat menjadi tolok ukur bagi pihak-pihak berwenang tentang sejauh mana upaya penjaminan keamanan perangkat yang sudah dilakukan selama ini beserta langkah strategis apa saja yang perlu dilakukan dalam mewujudkan standarisasi keamanan perangkat guna menjamin bahwa perangkat telekomunikasi yang digunakan aman dalam arti terjamin keamanan informasi yang dilewatkan melalui perangkat tersebut terutama perangkat telekomunikasi yang digunakan untuk keperluan hankamnas. Hasil penelitian menunjukkan belum ada regulasi yang mengatur standarisasi keamanan perangkat telekomunikasi untuk kebutuhan khusus. Selain itu belum ada penetapan secara eksplisit tentang lembaga yang berwenang dalam pengujian dan sertifikasi keamanan perangkat telekomunikasi terutama untuk kebutuhan khusus. Sejumlah regulasi yang mengatur secara spesifik bidang standarisasi keamanan perangkat telekomunikasi saat ini masih dalam proses penyusunan oleh instansi-instansi terkait.

2. Tinjauan Pustaka

2.1 Konsep pertahanan keamanan dalam kepentingan nasional

Robert Dorff (2004) menyatakan kepentingan suatu negara bangsa diperlihatkan dengan tingkah lakunya dalam membela, mengejar dan mempertahankan apa yang menjadi kepentingan dasarnya. Bagi banyak negara, kepentingan dasar suatu negara adalah menjaga wilayah, rakyat dan kedaulatannya. Semua unsur ini harus dipertahankan dan diperjuangkan agar tetap eksis dalam suatu negara. Mempertahankan kepentingan ini menjadi dasar dari tingkah laku suatu negara dalam berhubungan dengan negara lain dan aktor-aktor lain dalam sistem internasional, termasuk diantaranya melalui perang dan diplomasi (Dorff, 2004). Menurut Alan Gyngell & Michael Wesley (2007), kepentingan nasional adalah suatu konsep permanen yang menjadi orientasi kebijakan luar negeri suatu negara. Dengan kata lain konsep kepentingan nasional selalu menjadi landasan bagi semua pengambilan keputusan luar negeri dan juga dalam menganalisa kebijakan luar negeri (Gyngell & Wesley, 2007: 23). Kepentingan nasional merupakan tujuan jangka panjang dari suatu negara yang mengikat semua elemen pemerintah dan bangsa untuk mencapainya. Dengan demikian, bidang keamanan nasional juga diperluas dari dunia nyata ke dunia maya sehingga

muncul sebuah ancaman baru dalam sistem keamanan nasional yakni *Cyber War* dan masing-masing negara bersaing untuk memenangkan *Cyber War*. Kekuatan untuk menghancurkan ancaman *Cyber War* telah mencapai tahap langsung dan serius pada sistem keamanan nasional. Dalam tatanan globalisasi semua perangkat dapat mengakses informasi dimanapun sekaligus juga dapat diakses dari manapun. Kondisi ini memungkinkan penyalahgunaaninformasi yang dilewatkan melalui perangkat tersebut dengan menanamkan alat untuk mengambil maupun memodifikasi informasi untuk kepentingan tertentu.

2.2 Dasar pemikiran dan kebijakan TIK nasional

Perkembangan teknologi informasi dan komunikasi di dunia sudah sangat transparan dan memungkinkan setiap kejadian dan informasi yang ada di dunia ini dapat diakses cepat dan mudah seolah meniadakan batas antar negara. Kondisi ini memungkinkan penyalahgunaan informasi yang dilewatkan melalui perangkat tersebut dalam bentuk menyadap maupun memodifikasi informasi untuk kepentingan tertentu. yang mana hal tersebut menjadi suatu ancaman terhadap keutuhan negara. Oleh karenanya akan sangat berbahaya bagi suatu negara jika terus-menerus hanya menjadi pengguna dan menerima perangkat yang diproduksi dari luar (pihak asing) tanpa adanya jaminan standardisasi keamanan ataupun enkripsi yang dibuktikan dengan mengikuti peraturan nasional maupun internasional yang sudah ditetapkan oleh lembaga-lembaga berwenang.

2.3 Kebijakan standarisasi perangkat umum

Standarisasi sebagai suatu unsur penunjang pembangunan mempunyai peran penting dalam usaha optimasi pendayagunaan sumber daya dan seluruh kegiatan pembangunan. Perangkat yang terstandardisasi termasuk juga perangkat pembinaan dan pengawasan sangat berperan dalam peningkatan perdagangan dalam negeri dan internasional, pengembangan industri nasional, serta perlindungan terhadap pemakai (operator maupun masyarakat) dimana tujuan akhir kegiatan standardisasi adalah terwujudnya jaminan mutu. Sistem Standardisasi Nasional (SSN) merupakan dasar dan pedoman pelaksanaan setiap kegiatan standardisasi di Indonesia yang harus diacu oleh semua instansi teknis sesuai dengan Peraturan Pemerintah Nomor 15 Tahun 1991 tentang Standardisasi Nasional Indonesia dan Keputusan Presiden Nomor 12 Tahun 1991 tentang Penyusunan, Penerapan dan Pengawasan Standardisasi Nasional Indonesia. Dalam rangka mewujudkan pelaksanaan Sistem Standardisasi Nasional, juga dilakukan pengembangan dan penerapan standardisasi di bidang telekomunikasi.Kegiatan standardisasi di bidang telekomunikasi sepenuhnya ditangani oleh instansi teknis, dalam hal ini adalah Direktorat Jenderal Sumber Daya dan Perangkat Pos dan Informatika (SDPPI) yang dalam hal ini dilaksanakan oleh Direktorat Standardisasi SDPPI. Subsistem-subsistem atau kegiatan-kegiatan yang saling terkait satu sama lain dalam Sistem Standardisasi Nasional terdiri dari perumusan standardisasi, penerapan standardisasi, pembinaan dan pengawasan standardisasi, kerjasama dan informasi standardisasi, metrologi dan akreditasi. Tujuan dari kegiatan standardisasi pos dan telekomunikasi adalah :

- Pengamanan terhadap jaringan pos dan telekomunikasi, yang merupakan aset nasional.
- Menjamin interoperabilitas dan interkonektivitas berbagai perangkat dalam jaringan pos dan telekomunikasi.
- Memberi kesempatan munculnya industri manufaktur nasional.
- Memberi perlindungan terhadap para pengguna jasa (operator dan masyarakat) pos dan telekomunikasi.
- Mengendalikan mutu perangkat.
- Memberi kesempatan produk nasional bersaing di pasar global.

2.4 Kebijakan standarisasi perangkat khusus

Penerapan standar keamanan perangkat khusus biasanya diterapkan secara nasional, dalam cakupan suatu negara saja. Pengembangan standar keamanan perangkat khusus di Indonesia dibantu oleh badan-badan intelijen negara yang bersangkutan, antara lain:

- Badan Intelijen Negara (BIN),
- Badan Intelijen Strategis (BAIS), dan
- Lembaga Sandi Negara (Lemsaneg).

BIN dan Lemsaneg adalah Lembaga Pemerintah Nonkementerian (LPNK), yaitu lembaga negara di Indonesia yang dibentuk untuk melaksanakan tugas pemerintahan tertentu dari presiden, sedangkan BAIS berada di bawah komando Markas Besar Tentara Nasional Indonesia (Mabes TNI). Dari ketiga lembaga intelijen negara tersebut, yang memiliki fungsi yang berkaitan dengan keamanan sistem telekomunikasi militer adalah Lemsaneg.

Berdasarkan Peraturan Kepala Lembaga Sandi Negara Nomor OT.001/PERKA.122/2007 tentang Organisasi dan Tata Kerja Lembaga Sandi Negara, Lemsaneg mempunyai tugas melaksanakan tugas pemerintah di bidang persandian sesuai dengan ketentuan peraturan perundang-undangan yang berlaku. Dalam melaksanakan tugas tersebut sesuai OT.001/PERKA.122/2007, Lembaga Sandi Negara menyelenggarakan fungsi :

- Pengkajian dan penyusunan kebijakan nasional di bidang persandian;
- Koordinasi kegiatan fungsional dalam pelaksanaan tugas lemsaneg;
- Fasilitas dan pembinaan terhadap kegiatan instansi pemerintah di bidang persandian;
- Penyelenggaraan pembinaan pelayanan administrasi umum di bidang perencanaan umum, ketatausahan, organisasi dan tata laksana, kepegawaian, keuangan, kearsipan, hukum, persandian, perlengkapan dan rumah tangga.

2.5 Konsep Keamanan Teknologi Informasi dan Komunikasi Nasional

Konsep keamanan yang ada dalam ranah TIK memiliki cakupan yang sangat luas. Keamanan melingkupi empat aspek, yaitu *privacy/confidentiality*, *integrity*,*authentication*, dan *availability*. Selain keempat hal di atas, masih ada dua aspek lain yang juga sering dibahas, terutama dalam kaitannyadengan transasksi elektronik, yaitu *access control* dan *non-repudiation* (Garfinkel, 1995).

- *Privacy / Confidentiality*: Aspek terkait jaminan kerahasiaan isi dari informasi
- *Authentication*: Aspek yang menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses/memberikan informasi adalah betul-betul orang yang dimaksud
- *Integrity*: Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi
- *Accesibility*: Aspek iniberhubungan denganketersediaan informasi ketika dibutuhkan
- *Access control*\: Aspek ini berhubungan dengan cara pengaturan akses kepadainformasi
- *Non repudiation*: Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi

Seringkali masalah keamanan bahkan tidak terlalu diperhatikan, terutama apabila penerapan tindakan-tindakan keamanan mengganggu performansi sistem. Tidak jarang tindakan-tindakan keamanan dikurangi atau bahkan ditiadakan (Dowd & McHenry, 1998). Berdasarkan celah keamanan, keamanan dapat diklasifikasikan menjadi empat (David J. Icove, 1997), yaitu :

- Keamanan yang bersifat fisik (*physical security*). Keamanan fisik mencakup akses orang ke gedung, peralatan, dan media yang digunakan. Tidak menutup kemungkinan adalah kemudahan akses menuju berkas-berkas yang sudah dibuang yang mungkin memiliki informasi tentang keamanan, seperti catatan kata sandi (*password*) atau manual yang dibuang tanpa dihancurkan. *Wiretapping* atau hal-hal yang berhubungan dengan akses ke kabel atau komputer yang digunakan juga dapat dimasukkan ke

dalam kelas ini. *Denial of service* juga dapat dimasukkan ke dalam kelas ini. *Denial of service* adalah akibat yang ditimbulkan sehingga layanan yang seharusnya dapat diakses menjadi terhenti. Hal ini dapat terjadi misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan yang bukan berasal dari peminta layanan, sehingga pemberi layanan menjadi sibuk.

- Keamanan yang berhubungan dengan orang (*personel*). Klasifikasi ini mencakup identifikasi orang yang mempunyai akses, misalnya karyawan suatu organisasi. Seringkali kelemahan keamanan bergantung kepada manusia. Teknik "*social engineering*" sering digunakan oleh kriminal, misalkan dengan berpura-pura sebagai orang yang berhak mengakses informasi namun lupa kata sandi (*password*) yang dimilikinya.
- Keamanan dari data dan media serta teknik komunikasi (*communications*). Klasifikasi ini mencakup kelemahan-kelemahan yang terdapat di dalam perangkat lunak yang digunakan untuk mengelola data. Penyerang dapat memberikan virus atau trojan sehingga dapat mengumpulkan informasi (misalkan *password*) yang semestinya tidak berhak diakses.
- Keamanan dalam operasi, termasuk prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga termasuk prosedur setelah serangan (*post attack recovery*).

Secara spesifik, serangan terhadap keamanan (*security attack*) di dalam sistem informasi dapat dilihat dari fungsi peranan komputer atau jaringan computer sebagai penyedia informasi. Ada beberapa kemungkinan serangan (*attack*) yang dapat terjadi (William Stallings, 1995) dan (Rahardjo, 1999), diantaranya:

- *Interruption*: Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan (*availability*) dari sistem. Contoh serangan adalah "*denial of service attack*".
- *Interception*: Pihak yang tidak berwenang berhasil mengakses aset atau informasi. Contoh dari serangan ini adalah penyadapan (*wiretapping*).
- *Modification*: Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (*tamper*) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari web site dengan pesan-pesan yang merugikan pemilik web site.
- *Fabrication*: Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti e-mail palsu ke dalam jaringan komputer.

2.6 Penelitian sebelumnya

Dalam lingkup sistem telekomunikasi nasional umum/publik, penelitian mengenai keamanan perangkat jarang ditemukan. Penelitian yang umum ditemukan namun memiliki keterkaitan adalah penelitian mengenai keamanan informasi. Penelitian spesifik mengenai keamanan perangkat lebih sering dijumpai dalam sistem komunikasi yang umumnya digunakan dalam ranah pertahanan dan keamanan suatu negara, selanjutnya disebut sebagai sistem komunikasi khusus. Hal ini dapat dipahami mengingat perangkat komunikasi yang digunakan memiliki tingkat variasi yang rendah secara global, terlebih lagi dalam cakupan sebuah negara. Dalam sistem telekomunikasi khusus, keamanan sistem komunikasi sering dikenal dengan istilah spesifik COMSEC (*communication security*). Bidang penelitian COMSEC sangat spesifik mendalami perangkat yang digunakan. COMSEC dapat mencakup keamanan kripto (*cryptosecurity*), keamanan transmisi (*transmission security*/TRANSEC), dan keamanan fisik (*physical security*) perangkat telekomunikasi khusus. Beberapa kelompok peneliti dapat memiliki fokus penelitiannya sendiri, misalkan dalam hal keamanan emisi (*emmision security*). Contoh beberapa penelitian sebelumnya dapat ditemukan dalam bentuk penerapan mekanisme-mekanisme keamanan di atas pada perangkat telekomunikasi khusus. Pengembangan penelitian *low probability of interception*/LPI pada *transmission security* sering ditemukan pada perangkat radar. Radar LPI digunakan oleh personil militer untuk mendeteksi dan mengunci

target/lawan, namun radar itu sendiri sulit terdeteksi oleh perangkat deteksi pasif pihak lawan (Stove, 2004).

Contoh penerapan lainnya misalkan dapat dilihat dalam pengamanan sistem komunikasi satelit menerapkan metode-metode keamanan pada level transmisi serta dukungan saluran komunikasi yang aman seperti *virtual private network* (VPN) (J.M. Rodriguez Bejarano, 2012).

Penelitian mengenai deteksi ketidakamanan sistem biasanya melibatkan analisa trafik komunikasi yang terjadi. Banyak penelitan yang memiliki fokus kerawanan sistem seperti ini (Juslin, 2003; NargesArastouie, 2011).

Pada 2012 lalu media sempat diramaikan dengan hasil penemuan kerawanan (*vulnerabilities*) pada komponen elektronik yang sering dipakai dalam perangkat-perangkat militer. Penelitian di Universitas Cambridge menemukan hasil bahwa komponen chip yang digunakan oleh perangkat-perangkat sistem antariksa dan misil, pesawat tempur, sistem komputer penerbangan, sistem persenjataan, sistem radar, dan lainnya memiliki *backdoor* yang tersembunyi di dalamnya. *Backdoor* adalah fitur tambahan yang tak terdokumentasi yang sengaja dimasukkan ke dalam suatu komponen untuk memberikan fungsi-fungsi tambahan yang tersembunyi dari pihak pengguna (Woods, 2012).

Jejak *backdoor* ditemukan pada *system file* perangkat lunak pengembangan milik Actel, produsen chip *field-programmable gate arrays* (FPGA) yang banyak digunakan pada sistem-sistem militer. Bahaya dari *backdoor* ini memiliki efek yang signifikan karena FPGA ini dirancang untuk sistem dengan tingkat keamanan yang tinggi. Meskipun Actel mengklaim bahwa perangkatnya sangat aman karena tidak mungkin ada jalur fisik konfigurasi data dari luar chip FPGA tersebut, namun implementasi celah keamanan dengan cara-cara tersembunyi dan tertutup hanya untuk Actel membuat keamanan chip FPGA ini dipertanyakan. Jadi meskipun sejumlah perangkat sudah dilengkapi dengan fitur keamanan, potensi kebocoran keamanan tetap ada. Dalam sebuah tulisan yang membahas tentang evaluasi keamanan pada *smartphone*, ditemukan banyak celah keamanan di sejumlah aplikasi yang terpasang di dalam *smartphone* (Schrittwieser et al., 2012).

2.7 Penerapan standar keamanan TIK nasional

2.7.1 Perangkat Umum

Salah satu dasar penerapan standar keamanan perangkat umum di Indonesia dapat dilihat dalam Peraturan Menteri Komunikasi dan Informatika Nomor 18 Tahun 2014 tentang Sertifikasi Alat dan Perangkat Telekomunikasi. Sertifikasi yang dimaksud adalah dokumen yang menjelaskan bahwa suatu perangkat telah melalui serangkaian proses pengujian. Adanya sertifikat ini memastikan bahwa perangkat bisa terhubung dan berkomunikasi dengan perangkat atau sistem yang sudah ada tanpa mengganggu dan terganggu oleh sistem komunikasi lainnya. Peraturan ini menjelaskan bahwa penerbit sertifikasi perangkat adalah Lembaga Sertifikasi, Direktorat Standarisasi Perangkat Pos dan Informatika. Untuk memperoleh sertifikat tersebut, perangkat yang diajukan harus melalui pengujian yang dilaksanakan oleh pelaksana pengujian (Balai Uji). Balai Uji yang telah ditetapkan adalah Balai Besar Pengujian Perangkat Telekomunikasi (BBPPT) Kementerian Komunikasi dan Informatika dan *Innovation and Design Center* (IDEC) PT. Telekomunikasi Indonesia.

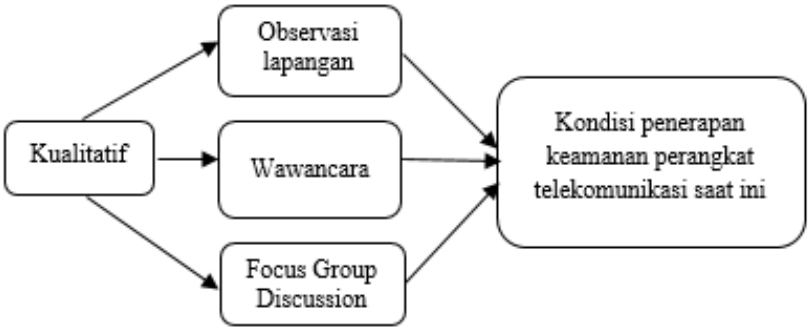
2.7.2 Perangkat Khusus

Penerapan standard keamanan perangkat khusus memiliki standard yang tidak terbuka. Standard keamanan untuk perangkat militer biasanya ditetapkan sendiri-sendiri secara khusus (*proprietary*) oleh pihak-pihak yang berkepentingan. Dengan adanya persyaratan keamanan telekomunikasi militer yang sangat ketat, standard masing-masing pihak yang berkepentingan umumnya tidak diizinkan untuk diketahui pihak lain, sehingga dapat dikatakan standard keamanan yang diberlakukan secara internasional hampir

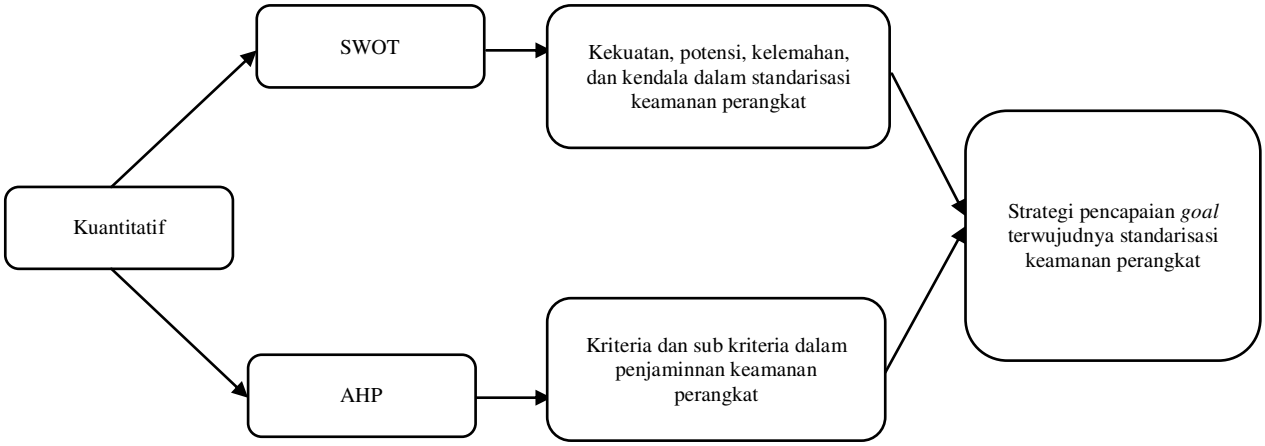
tidak ada. Beberapa standard yang mungkin ada biasanya berupa standard komunikasi umum antar pihak militer satu dengan pihak militer yang lainnya di mana tidak terdapat pertukaran informasi yang sangat rahasia pada komunikasi yang sedang berlangsung. Penerapan standard keamanan perangkat militer biasanya diterapkan secara nasional, dalam cakupan suatu negara saja. Pengembangan standard keamanan perangkat militer biasanya dibantu oleh badan-badan intelijen negara yang bersangkutan. Di Indonesia, peralatan-peralatan komunikasi militer yang digunakan oleh tiap angkatan (Angkatan Darat, Angkatan Laut, dan Angkatan Udara) dikatakan disertifikasi oleh Badan Penelitian dan Pengembangan masing-masing angkatan. Meskipun demikian, Lembaga Sandi Negara (Lemsaneg) memiliki rencana untuk mewajibkan penerapan standar keamanan perangkat. Saat ini Lemsaneg telah memiliki bagian Sub-direktorat Akreditasi dan Sertifikasi yang melakukan sertifikasi perangkat-perangkat dengan fitur-fitur kemanan. Lemsaneg memiliki rencana untuk mewajibkan sertifikasi perangkat khusus dengan mengusahakan undang-undang mengenai sertifikasi tersebut pada 2016 untuk mengatur persyaratan teknis perangkat-perangkat sandi.

3. Metode Penelitian

Penelitian ini dilakukan menggunakan metode campuran meliputi kuantitatif dan kualitatif. Metode kuantitatif yang dipakai adalah AHP (*Analytical Hierarchy Process*) dan SWOT (*Strength, Weakness, Opprtunity, Threat*). AHP digunakan untuk mengetahui faktor atau kriteria yang terkait dengan standarisasi keamanan perangkat yang meliputi *Standard of Procedure*, jaminan keamanan dari vendor, kualifikasi unggul operator/vendor, kelembagaan, dan audit beserta sub kriteria dari setiap faktor tersebut yang meliputi kebijakan, pembinaan, dan penegakan hukum. Berdasarkan bobot nilai kriteria dan sub kriterianya dapat diketahui prioritas kriteria yang berpengaruh signifikan untuk implementasi standardisasi keamanan perangkat dan pendekatan sub kriteria yang paling sesuai digunakan apakah pendekatan kebijakan, pembinaan atau penegakan hukum. Metode SWOT digunakan untuk mengidentifikasi kelebihan dan kekurangan yang dihadapi saat ini dalam penerapan keamanan perangkat. Berdasarkan hasil identifikasi, dapat dirumuskan model strategi yang sesuai dilakukan untuk mencapai *goal* terwujudnya standardisasi keamanan perangkat. Metode kualitatif dilakukan melalui observasi lapangan, wawancara mendalam, dan *focus group discussion* untuk mengetahui gambaran kondisi penerapan keamanan perangkat saat ini. Metode campuran ini dilakukan karena melalui penelitian ini ingin diperoleh gambaran tentang kondisi penerapan keamanan perangkat telekomunikasi saat ini dan juga identifikasi potensi dan kendala yang dihadapi sehingga dapat dijadikan dasar untuk merumuskan strategi penanganan yang tepat guna mencapai *goal* terwujudnya standarisasi keamanan.



Gambar 1. Metode kualitatif



Gambar 2. Metode kuantitatif

Teknik penentuan informan/narasumber berdasarkan faktor keterlibatan dalam isu yang diangkat dan ahli dalam bidang tersebut. Informan/narsumber dalam pendekatan kualitatiif adalah para pelaku industri TIK seperti operator jaringan seluler, vendor perangkat telekomunikasi, akademisi serta instansi pemerintah di Indonesia. Pemilihan lokasi penelitian yakni di Jakarta, Bandung dan Batam mempertimbangkan lokasi keberadaan para pelaku industri TIK dan balai-balai pengujian perangkat yang tersedia. Analisa data dimulai dengan dugaan tentang keadaan masa sekarang meliputi ekosistem perangkat telekomunikasi, potensi kebocoran keamanan, proyeksi para pakar dan perkiraan terjadinya tingkat ketergantungan terhadap vendor asing yang semakin tinggi serta pemberdayaan lembaga uji untuk penerapkan standard keamanan.

4. Hasil dan Pembahasan

4.1 Penerapan Standard Keamanan, Termasuk Audit dan Kelengkapan Pengujian Perangkat TIK

4.1.1 Perangkat Umum

Penerapan standard keamanan perangkat TIK untuk kebutuhan umum selama ini banyak menggunakan standard internasional, seperti diantaranya: ISO/IEC, ETSI, ITU, COBIT 5, CC (*Common Criteria*) dan standard pabrikan dari produsen perangkat. Selain standard tersebut, industri juga membuat kebijakan (*policy*) internal untuk pengamanan perangkat dan sistem yang dimiliki, hal ini dilakukan oleh industri karena dirasa lebih menjamin keamanan perangkat TIK. Sejumlah industri telah melakukan audit internal maupun eksternal (audit terkait sertifikasi sepeti ISO, dsb) namun belum ada kewajiban pelaporan hasil audit kepada pemerintah. Keberadaan fasilitas pengujian juga masih sangat terbatas baik jumlah maupun kelengkapan peralatan uji. Hasil ini menunjukkan bahwa untuk perangkat TIK untuk kebutuhan umum sudah memiliki standard baku akan tetapi masih diperlukan upaya lanjutan terkait kelengkapan fasilitas pengujian dan pelaporan hasil audit berkala kepada pemerintah.

4.1.2 Perangkat Khusus

Penerapan standard keamanan perangkat TIK untuk kebutuhan khusus selama ini mengikuti standard bawaan vendor perangkat TIK dan kebijakan internal pengamanan informasi di masing-masing instansi. Perangkat TIK untuk pengiriman informasi rahasia (*confidential*) seperti peralatan sandi, mengikuti prosedur dari Lemsaneg yang mengacu pada standard internasional ISO 19790 dan ISO 24759 tentang standard keamanan peralatan sandi/kriptografi. Keberadaan fasilitas pengujian dan audit keamanan perangkat masih sangat terbatas baik jumlah maupun kelengkapan peralatan uji. Hasil ini menunjukkan perangkat TIK untuk kebutuhan khusus belum memiliki standard keamanan tersendiri yang terpisah dengan standard keamanan perangkat untuk kebutuhan umum.

4.2 Status Regulasi Penerapan Standard Keamanan Perangkat TIK

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang

Nomor 3 Tahun 2002 tentang Pertahanan Negara, Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, Peraturan Menteri Kominfo Nomor 18 Tahun 2014 tentang Sertifikasi Alat dan Perangkat Telekomunikasi, Peraturan Kepala Lembaga Sandi Negara Nomor 9 Tahun 2010 tentang Pedoman Sertifikasi Peralatan Sandi, Peraturan Menteri Komunikasi dan Informatika Nomor 1 Tahun 2015 tentang Perubahan atas Peraturan Menteri Kominfo Nomor 18 Tahun 2014 adalah sejumlah regulasi yang terkait pertahanan dan keamanan dan juga beberapa mengatur tentang sertifikasi alat dan perangkat. Namun regulasi-regulasi tersebut belum secara spesifik memuat standarisasi keamanan perangkat termasuk level-level standar keamanannya baik untuk kebutuhan umum maupun kebutuhan khusus sehingga dibutuhkan peraturan perundangan yang secara khusus dan spesifik memuat pengaturan standar keamanan perangkat tersebut.

4.3 Peran Regulator dalam Mengatur dan mengawasi Penerapan Standar Keamanan Perangkat TIK Nasional

Lembaga sandi negara sudah memiliki unit tersendiri untuk melakukan pengujian dan sertifikasi perangkat TIK dengan fitur-fitur keamanan khusus yang digunakan untuk lingkungan pemerintahan meskipun belum ada standar baku secara nasional. Lemsaneg sudah menyusun acuan internal untuk pengujian dan sertifikasi keamanan perangkat yang mengacu standar internasional ISO 19790 tentang aspek keamanan yang harus dipenuhi oleh modul kriptografi, ISO 24759 tentang metode pengujian untuk modul kriptografi serta berdasarkan pada pengalaman badan litbang Lemsaneg selama ini dalam menangani bidang kriptografi untuk instansi pemerintah. Sementara Kementerian Kominfo juga memiliki unit tersendiri untuk pengujian dan sertifikasi perangkat TIK namun hanya mencakup keamanan perangkat di sisi kesehatan bukan dari sisi keamanan informasi. Sejumlah instansi pemerintah yang belum memiliki fasilitas pengujian sendiri, maka unit yang berwenang menangani keamanan perangkat di internal instansi masing-masing berkoordinasi dengan Lemsaneg untuk pengujian dan sertifikasi perangkat TIK untuk keperluan yang bersifat rahasia (*confidential*) atau kebutuhan khusus. Jadi dalam hal ini regulator memiliki peran yang vital dalam menyusun kebijakan sekaligus pengawasan dalam bidang penerapan standardisasi keamanan perangkat.

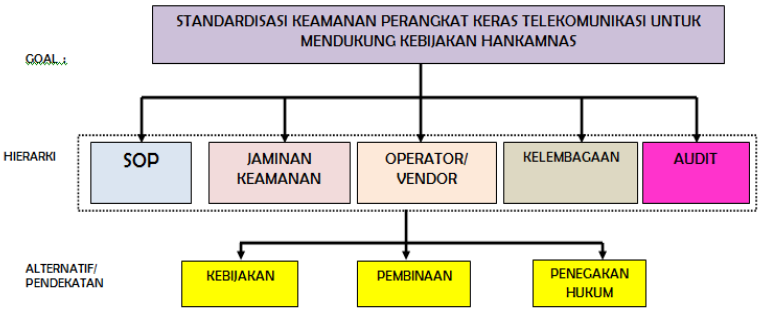
4.4 Kendala yang dihadapi dalam menjamin keamanan perangkat TIK untuk kebutuhan umum maupun kebutuhan khusus

Sejumlah kendala yang dihadapi terkait penjaminan keamanan perangkat telekomunikasi diantaranya masih minimnya regulasi nasional dalam penerapan standard dan prosedur serta jaminan keamanan perangkat TIK yang dapat diikuti oleh pemerintah dan industri, keterbatasan tenaga ahli lokal dalam bidang keamanan informasi, keterbatasan fasilitas balai uji keamanan perangkat yang dapat mendukung secara teknis regulasi yang telah dan akan ditetapkan, ketergantungan terhadap vendor asing masih tinggi, kolaborasi serta sinergi antar pihak terkait baik industri maupun pemerintah yang masih minim.

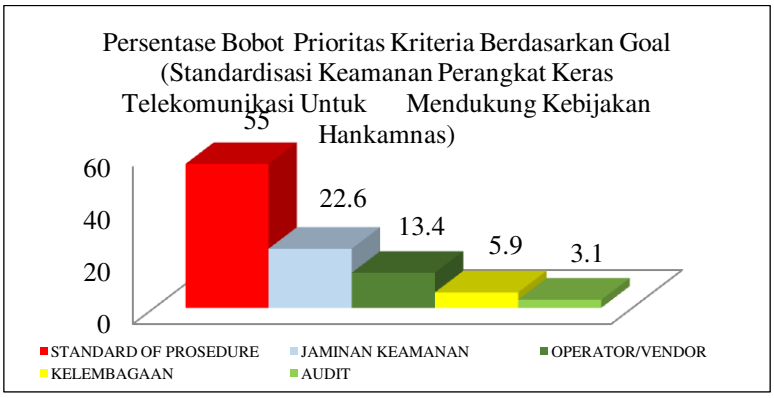
4.5 Analisis AHP dan SWOT

4.5.1 AHP

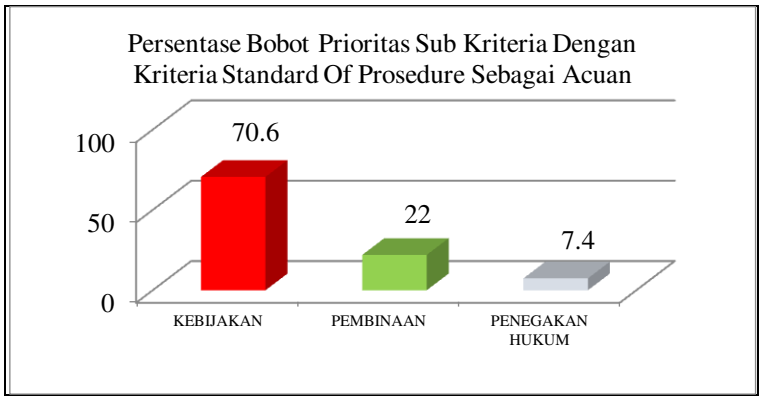
Struktur AHP yang digunakan pada studi ini diperlihatkan pada Gambar 3 dan Hasilnya disajikan dalam bentuk grafik pada Gambar 4 sampai dengan Gambar 9. Berdasarkan grafik pada gambar 4 dapat dilihat bahwa kriteria atau faktor *Standard of Procedure*, jaminan keamanan perangkat dari vendor, dan kualifikasi unggul operator/vendor merupakan tiga faktor yang signifikan dalam mewujudkan standarisasi keamanan perangkat telekomunikasi khususnya untuk mendukung kebijakan hankamnas dengan bobot nilai berturut-turut 55%, 22.6%, dan 13.4%.



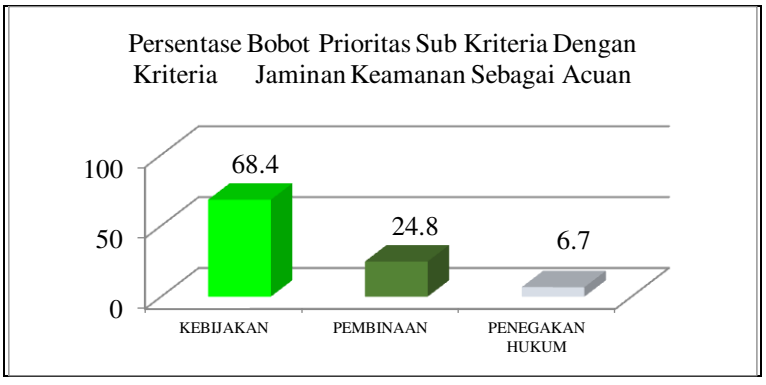
Gambar 3. Analisis AHP



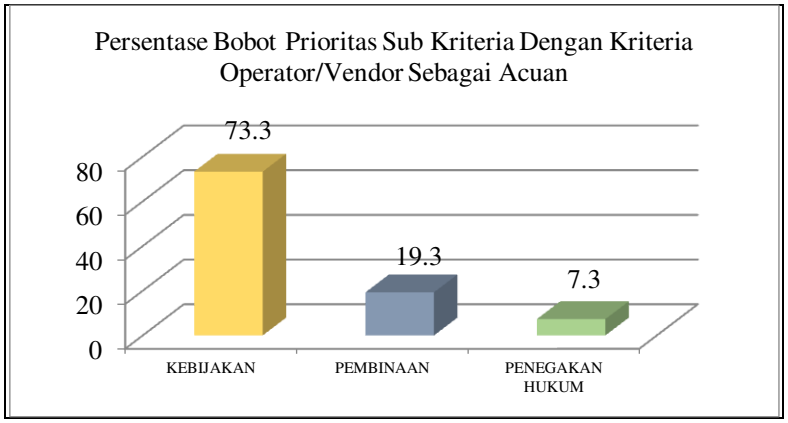
Gambar 4. Hasil AHP-Persentase bobot kriteria



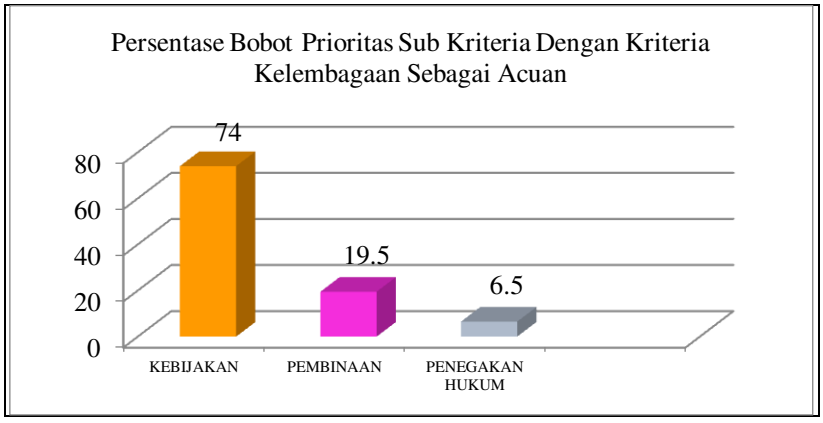
Gambar 5. Bobot sub kriteria dengan kriteria SOP sebagai acuan



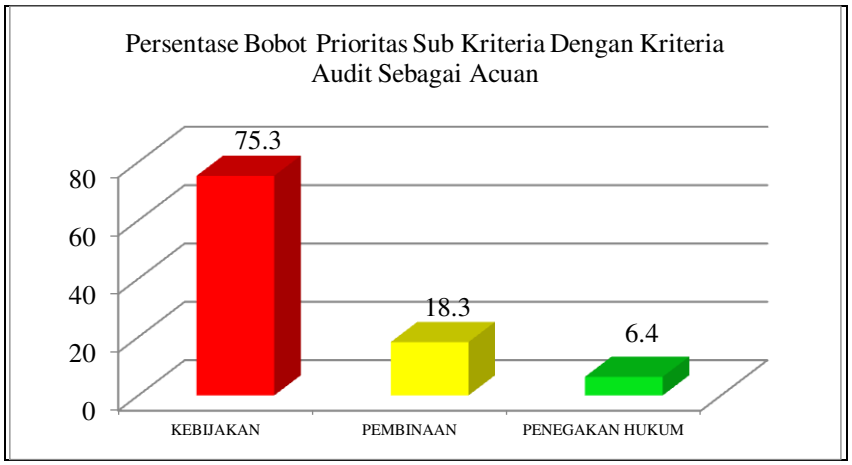
Gambar 6. Bobot sub kriteria dengan kriteria jaminan keamanan sebagai acuan



Gambar 7. Bobot sub kriteria dengan kriteria kualifikasi industri sebagai acuan



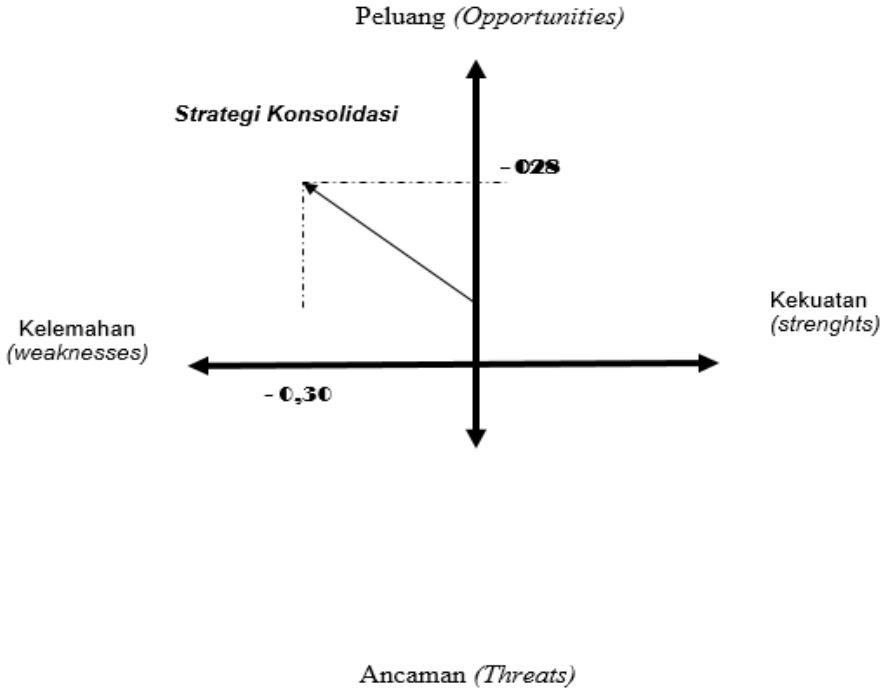
Gambar 8. Bobot sub kriteria dengan kriteria kelembagaan sebagai acuan



Gambar 9. Bobot sub kriteria dengan kriteria audit sebagai acuan

Dari gambar 5 hingga gambar 9 tampak bahwa untuk mewujudkan standarisasi keamanan perangkat telekomunikasi untuk setiap kriteria atau faktor tersebut, pendekatan kebijakan mendapatkan bobot nilai paling tinggi. Dengan kata lain dalam mewujudkan standarisasi keamanan perangkat telekomunikasi baik melalui penyusunan SOP, jaminan keamanan dari vendor, kualifikasi operator/vendor, maupun kelembagaan dan audit dibutuhkan pendekatan kebijakan dimana dalam hal ini adalah keberadaan regulasi sebagai dasar hukum dalam mewujudkan upaya standarisasi keamanan perangkat telekomunikasi.

4.5.2 SWOT



Gambar 10. Hasil analisa SWOT

Melalui analisis SWOT diidentifikasi faktor internal dan eksternal dalam pencapaian *goal* standarisasi keamanan perangkat telekomunikasi yang meliputi kekuatan, kelemahan, potensi, dan ancaman yang terbagi dalam empat kuadran sebagai tertera dalam gambar 10. Kuadran I berada pada daerah kanan atas, kuadran II berada pada daerah kanan bawah, kuadran III berada pada daerah kiri bawah sementara kuadran IV berada pada daerah kiri atas. Berdasarkan hasil perhitungan SWOT diperoleh bobot nilai untuk perbandingan kekuatan – kelemahan sebesar - 0.3 sementara bobot nilai perbandingan peluang – ancaman sebesar 0.28 yang berarti berada pada kuadran IV yang berarti bahwa dalam upaya mencapai goal standarisasi keamanan perangkat masih banyak ditemukan kelemahan dan tantangan. Oleh karena itu berdasarkan hasil tersebut maka dalam diagram tersebut, strategi yang paling mungkin dilakukan bagi dalam penanganan komprehensif standardisasi keamanan telekomunikasi khususnya di bidang Pertahanan dan Keamanan Nasional yakni strategi *"konsolidasi"* yang berada di kuadran IV. Strategi tersebut mempersyaratkan upaya yang mungkin dapat dilakukan yakni memanfaatkan dan mengoptimalkan peluang yang ada untuk meminimalkan kelemahan-kelemahan yang dimiliki.

5. Simpulan dan saran

5.1. Simpulan

Kesimpulan dari penelitian ini adalah upaya penerapan standar keamanan perangkat telekomunikasi yang ada saat ini hanya mencakup perangkat untuk kebutuhan umum sementara perangkat untuk kebutuhan khusus belum memiliki standar keamanan tersendiri. Saat ini regulasi bidang standardisasi keamanan perangkat telekomunikasi masih belum memadai terutama yang ditujukan bagi perangkat telekomunikasi untuk kebutuhan khusus. Sejumlah kendala yang dihadapi terkait penjaminan keamanan perangkat telekomunikasi seperti keterbatasan tenaga ahli lokal dalam bidang keamanan informasi, keterbatasan fasilitas balai uji keamanan perangkat yang dapat mendukung secara teknis regulasi yang telah dan akan ditetapkan, ketergantungan terhadap vendor asing masih tinggi, dan kolaborasi serta sinergi antar pihak terkait baik industri maupun pemerintah yang masih minim. Pemerintah sebagai regulator memiliki peran yang vital sebagai penyusun kebijakan sekaligus pengawasan dalam bidang penerapan standarisasi

keamanan perangkat. Dalam mencapai *goal* standarisasi keamanan perangkat telekomunikasi khususnya untuk menunjang kebijakan hankamnas masih banyak diperlukan upaya lebih lanjut untuk mewujudkannya.

5.2. Saran

Saran yang dapat diberikan berdasarkan hasil penelitian ini yakni instansi-instansi pemerintah perlu segera menyusun *roadmap* terkait implementasi standard keamanan perangkat telekomunikasi meliputi sejumlah tahapan yakni penyusunan dan penetapan regulasi yang spesifik mengatur standardisasi keamanan perangkat, penetapan lembaga yang mempunyai otoritas dalam menguji dan mensertifikasi keamanan perangkat, penyusunan pedoman teknis yang memuat sertifikasi dan audit keamanan perangkat. Selain itu diperlukan juga penguatan kemitraan dengan industri nasional ataupun lembaga standardisasi internasional untuk perbaikan standar keamanan TIK dan mempercepat *transfer of technology* selama didasarkan atas prinsip-prinsip saling menghargai kedaulatan antar negara. Penguatan kolaborasi dan sinergi antar instansi pemerintah misalnya dengan pembentukan dewan keamanan informasi yang beranggotakan instansi pemerintah yang berwenang seperti Kementerian Kominfo, Lemsaneg, BIN, BAIS, Polri, TNI, Kementerian Pertahanan dan sebagainya. Hasil penelitian diharapkan dapat menjadi acuan bagi penelitian selanjutnya, dengan lebih memfokuskan permasalahan pada aspek-aspek yang terkait dengan tahapan dalam penyusunan *roadmap*.

6. Ucapan Terima Kasih

Ucapan terima kasih dan penghargaan yang tinggi penulis sampaikan kepada bapak Ian Yosef dan bapak Daniel Wiyogo dari ITB, bapak Herdis Herdiansyah dari Universitas Indonesia, bapak Ahmad Hasyim dari Puslitbang Aptika IKP Kementerian Kominfo yang telah bersedia memberikan kontribusinya dalam pelaksanaan penelitian hingga selesai. Ucapan terima kasih juga penulis sampaikan kepada Puslitbang SDPPI Kementerian Kominfo sebagai pihak yang memfasilitasi penelitian ini dari tahap awal hingga selesainya penelitian ini.

Daftar Pustaka

David J. Icove. (1997). Collaring the cybercrook: an investigator's view. *IEEE Spectrum*, 31–36.

Dowd, P. W., & McHenry, J. T. (1998). Network Security: It's Time To Take It Seriously. *IEEE Computer*, *September*, 24–28.

Garfinkel, S. (1995). *PGP: Pretty Good Privacy*. O'Reilly & Associates,Inc.

J.M. Rodriguez Bejarano. (2012). Security in IP satellite networks: COMSEC and TRANSEC integration aspects. In *Security in IP satellite networks: COMSEC and TRANSEC integration aspects*. The Sixth Advanced Satellite Multimedia Systems Conference.

Juslin, J. (2003). Automatic backdoor analysis with a network intrusion detection system and an integrated service checker. Information Assurance Workshop.

Kiblat.mht. (2015). http://www.kiblat.net/2015/02/25/dan-inggris-retas-ponsel-seluruh-dunia-ini-10-hal-yang-perlu-anda-tahu/.

NargesArastouie, E. S. dan. (2011). Backdoor detection system using artificial neural network and genetic algorithm.

Paryati. (2008). Keamanan Sistem Informasi. *Seminar Nasional Informatika 2008*.

Rahardjo, B. (1999). *Keamanan Sistem Informasi Berbasis Internet*. Bandung: PT Insan Komunikasi / Infonesia.

Richardus, Eko, & Indrajit. (2011). MANAJEMEN KEAMANAN INFORMASI DAN INTERNET.

Schrittwieser, S., Fr¨uhwirt, P., Kieseberg, P., Leithner, M., Mulazzani, M., Huber, M., & Weippl, E. (2012). Guess Who's Texting You? Evaluating the Security of Smartphone Messaging Applications. *SBA Research gGmbH*.

Stove, A. G. (2004). Low probability of intercept radar strategies. *IEEE Proceedings on Radar, Sonar and Navigation*, *151*(5).

Wamala, F. (2011). ITU National Cyber Security Strategy Guide. ITU.

Wicaksono, N. (2007). AUREN: Sistem Pengamanan Smartphone dengan Penghapusan Informasi Berharga dan Pengiriman Informasi untuk pelacakan otomatis. Bandung.

William Stallings. (1995). *Network and Internetwork Security*. PrenticeHall.

Woods, S. S. dan C. (2012). Breakthrough silicon scanning discovers backdoor in military chip.