UNIVERSITAS PERTAHANAN INDONESIA

POLA KETERBUKAAN INFORMASI BIDANG PERTAHANAN DI INDONESIA SEBAGAI ANCAMAN NONTRADISIONAL

TESIS

Diajukan sebagai salah satu syarat untuk memperoleh
Gelar Magister Sains di Bidang Pertahanan

FAUZIA GUSTARINA CEMPAKA TIMUR
120130102008

PROGRAM STUDI PEPERANGAN ASIMETRIS
FAKULTAS STRATEGI PERTAHANAN

BOGOR
FEBRUARI 2015

LEMBAR PENGESAHAN

Tesis ini diajukan oleh:

Nama	:	Fauzia Gustarina Cempaka Timur
NPM	:	120130102008
Program Studi	:	Peperangan Asimetris
Judul Tesis	:	Pola Keterbukaan Informasi Bidang Pertahanan di Indonesia sebagai Ancaman Nontradisional

Telah berhasil dipertahankan dihadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Magister Sains bidang Ilmu Pertahanan pada Program Studi Peperangan Asimetris, Fakultas Strategi Pertahanan Universitas Pertahanan Indonesia.

DEWAN PENGUJI

Pembimbing I : Laksma TNI (Purn) Iwan Kustiyawan, M.M ( )

Pembimbing II : Riefqi Muna, Ph.D ( )

Penguji I : Kol. Lek Dr. Arwin D.W. Sumari, M.T. ( )

Penguji II : Kol. Lek St. Haposan Simatupang, M.Si (Han) ( )

Penguji III : Kol. Sus Prayitno M.T.I. ( )

Ditetapkan di : Bogor

Tanggal : 26 Februari 2015

PERNYATAAN

Dengan ini saya menyatakan bahwa dalam tesis ini tidak terdapat karya atau bagian karya yang pernah diajukan untuk memperolah gelar kesarjanaan jenjang apapun di suatu Perguruan Tinggi; dan sepanjang pengetahuan saya juga tidak terdapat istilah, frasa, kalimat, paragraf, subbab, atau bab dari karya yang pernah ditulis atau diterbitkan; kecuali yang secara tertulis dirujuk dalam naskah ini dan disebutkan dalam Daftar Referensi.

Apabila di kemudian hari terbukti bahwa terdapat plagiat dalam tesis ini, saya bersedia menerima sanksi sesuai ketentuan peraturan dan undang-undang yang berlaku.

Bogor, 26 Februari 2015

Fauzia Gustarina Cempaka Timur

PERNYATAAN PERSETUJUAN PUBLIKASI
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Pertahanan Indonesia, saya yang bertanda tangan di bawah ini:

Nama : Fauzia Gustarina Cempaka Timur
NPM : 120130102008
Program Studi : Peperangan Asimetris (PA)
Fakultas : Strategi Pertahanan
Jenis karya : Tesis

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pertahanan Indonesia **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul:

POLA KETERBUKAAN INFORMASI BIDANG PERTAHANAN DI INDONESIA SEBAGAI ANCAMAN NONTRADISIONAL

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Pertahanan Indonesia berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*) merawat, dan memublikasikan Tugas Akhir saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik Hak Cipta/Karya Intelektual dari tesis ini.

Demikian pernyataan ini saya buat dengan kesadaran penuh tanpa paksaan dari pihak manapun.

Bogor, 26 Februari 2015
Yang menyatakan,

Fauzia Gustarina Cempaka Timur

KATA PENGANTAR

Segala puji bagi Allah SWT atas segala rahmat, rezeki dan nikmat-Nya yang tak pernah habis bagi penulis. Berbagai petunjuk dan perlindungan yang diberikan oleh Allah SWT – lah yang telah mendampingi saya selama pengerjaan tesis ini. dengan judul:

"POLA KETERBUKAAN INFORMASI BIDANG PERTAHANAN DI INDONESIA SEBAGAI ANCAMAN NONTRADISIONAL"

Penelitian tesis ini dapat diselesaikan berkat bantuan dan dukungan berbagai pihak baik yang terkait langsung maupun tidak langsung. Atas bantuan dan dukungan yang telah diberikan penulis mengucapkan terima kasih. Namun, terima kasih yang besar atas selesainya penelitian ini disampaikan penulis kepada:

1. Laksamana Madya TNI Dr. Desi Albert Mamahit, M. Sc., selaku Rektor Universitas Pertahanan Indonesia yang telah banyak memberikan dukungan bagi mahasiswa dalam menyelesaikan pendidikan.
2. Mayor Jenderal TNI (Mar) Dr. Syaiful Anwar, M. Bus., MA., selaku Dekan Fakultas Strategi Pertahanan yang telah memberikan motivasi kepada penulis dalam menjelaskan proses penyusunan tesis.
3. Laksamana Pertama TNI (Purn) Iwan Kustiyawan SIP., M.M., dan Riefqi Muna, Ph.D selaku dosen pembimbing yang telah sabar memberikan masukan, saran, dan arahan yang membangun untuk penulis dalam penelitian dan penyusunan tesis ini.
4. Kolonel Elektronika Haposan Simatupang, M. Si (Han), sebagai Ketua Program Studi Peperangan Asimetris atas saran beliau dalam percepatan penulisan ini.
5. Para narasumber yang dapat diwawancarai dan memberikan bantuan dalam proses pengambilan data-data penting untuk mendukung dalam penyusunan penelitian.
6. Ayah tercinta Mayor Jenderal Imam Edy Mulyono, SIP, M.Sc., dan Ibun tersayang Ir. Dwiretnani Hesti M., yang mengajarkan untuk selalu

berusaha yang terbaik dalam mengerjakan sesuatu, termasuk pengerjaan tesis ini dan selalu menjadi inspirasi bagi penulis dalam menjalani hari-hari.

7. Melati, *a mother, a sister, a best friend.* Adikku Iron, Kakak Iparku Mas Yogi dan gadis-gadis kecil Intania dan Diba yang selalu memberikan motivasi, semangat, dan senyum keceriaan pada penulis di tengah kesibukan penulis dalam menyelesaikan tesis.

8. Alvin Thias Aditya, SIP., *A very good man,* dan Rizka Fiani Prabaningtyas, SIP., *A good woman,* sebagai orang yang dikirimkan Allah SWT sebagai sahabat yang selalu dekat di hati. Terimakasih atas doa yang hadir dalam kesulitan dan kesenangan saat mengerjakan tesis ini.

9. Rekan-rekan Program Studi Peperangan Asimetris Cohort 02, terutama kepada Sarwa, Binar, dan Mbak Ani yang telah menjadi sahabat dalam berdiskusi, bercerita, bercengkrama, dan berjuang selama perkuliahan maupun selama pengerjaan tesis ini. Juga untuk Mas Andre dan Bang Mexa yang selalu memberikan perspektif baru dan menarik sehingga tesis ini berhasil diselesaikan. Semoga kita semua semakin sukses!

Dengan keterbatasan saya selaku peneliti, penelitian tesis ini masih jauh dari sempurna. Oleh karena itu, saya mengharapkan kritik dan saran membangun dari semua pihak yang terkait dengan penelitian ini. Akhir kata, semoga hasil penelitian dapat bermanfaat bagi perkembangan ilmu khususnya dalam bidang peperangan asimetris (*asymmetric warfare*) dan dapat memberikan kontribusi positif dalam keterbukaan dan keamanan informasi pertahanan di Indonesia sebagai bentuk menghadapi ancaman nontradisional.

Bogor, 26 Februari 2015

Fauzia Gustarina Cempaka Timur
NPM. 120130102008

ABSTRAK

Nama : Fauzia Gustarina Cempaka Timur
Program Studi : Peperangan Asimetris
Judul : Pola Keterbukaan Informasi Bidang Pertahanan di Indonesia Sebagai Ancaman Nontradisional

Penelitian ini menganalisis dan meninjau pola keterbukaan informasi bidang pertahanan Indonesia dan dampaknya terhadap posisi Indonesia dalam peperangan informasi dihadapkan pada ancaman nontradisional. Penelitian dilakukan dengan metode interpretasi-naratif analisis kualitatif. Pengumpulan data dilakukan melalui teknik kepustakaan dan *purposive sampling* melalui observasi dan wawancara. Berdasarkan hasil penelitian menunjukan, Kementerian Komunikasi dan Informatika serta Kementerian Pertahanan menerapkan Pola Pendekatan Defensif untuk menjaga pola keterbukaan informasi pertahanan di Indonesia. Meski begitu, sistem keamanan informasi pertahanan yang berjalan selaras dengan pola keterbukaan informasi belum cukup optimal dalam melindungi keamanan informasi pertahanan yang membuat pola keterbukaan Indonesia saat ini rawan sebagai ancaman nontradisional

Kata Kunci : Pola Keterbukaan Informasi, Informasi Pertahanan, Keunggulan Informasi, Ancaman Nontradisional.

Name : Fauzia Gustarina Cempaka Timur
Study Program : Asymmetric Warfare
Judul : Defense Information Openness Pattern in Indonesia as Nontraditional Threat

ABSTRACT

This research analyzes and reviews the pattern of defense information openness and its impact on Indonesia's position in information warfare challenged with nontraditional threats. Study carried out by the method of interpretation-narrative qualitative analysis. Data collected over literatures and purposive sampling techniques through observation and interviews. Based on the results of the study showed, the Ministry of Communications and Information and the Ministry of Defense implement Defensive Approach in the pattern of defense information openness in Indonesia. However, information security defense system that goes along with the pattern of information openness is not enough to protect the security of defense information that makes the pattern of openness in Indonesia is prone as nontraditional threats.

Keywords : The Pattern of Information Openness, Defense Information, Information Supremacy, Nontraditional Threat.

DAFTAR ISI

HALAMAN JUDUL ……..... i
LEMBAR PENGESAHAN ……... ii
LEMBAR PERNYATAAN ORIGINALITAS …… iii
LEMBAR PERSETUJUAN PUBLIKASI KARYA ILMIAH …….. iv
KATA PENGANTAR …… v
ABSTRAK …… vii
DAFTAR ISI …… viii
DAFTAR GAMBAR ……. xi
DAFTAR LAMPIRAN ……. xii
DAFTAR SINGKATAN .....…. xiii

1 PENDAHULUAN ……. 1
1.1. Latar Belakang ……. 1
1.2. Rumusan Masalah …….. 6
1.3. Tujuan Penelitian dan Signifikansi Penelitian ..…….. 7
1.4. Manfaat Penelitian ……... 7
1.5. Ruang Lingkup dan Gambaran Desain Penelitian….. 8

2 TINJAUAN PUSTAKA, KERANGKA PEMIKIRAN, DAN PENELITIAN RELEVAN…….. 11
2.1. Tinjauan Pustaka ……..…….…….. 11
2.1.1. Pola……..... 12
2.1.2. Teori Informasi ..……..…… 13
2.1.2.1. Keterbukaan Informasi……... 15
2.1.2.2. Resiko Ancaman pada Sistem Informasi……. 16
2.1.2.3. Teori Keunggulan Informasi…….……..…….. 17
2.1.3. Konsep Ancaman Nontradisional…….. 19
2.1.4. Teori Partisipasi Masyarakat ……..…….. 20
2.2. Kerangka Pemikiran.. ……..……..…….. 22
2.3. Hasil Penelitian yang Relevan……. 25

3 METODOLOGI PENELITIAN 29
3.1. Sumber Data/Subjek/Objek Penelitian…..…… 29
3.2. Desain Penelitian .....…… 30
3.3. Teknik Pengumpulan Data…….....…….. 31
3.3.1. Studi Pustaka (*Library Research)*..... 31
3.3.2. Wawancara Mendalam (*In-Depth Interview)*……. 31
3.4. Teknik Penentuan Informan (Narasumber)...…..... 32
3.5. Prosedur Pengolahan Data…..…….....…..…… 32

4 DATA DAN ANALISIS PENELITIAN……. 34
4.1. Hasil Penelitian…….....……..…. 34
4.1.1. Gambaran Umum Pola Keterbukaan Informasi di Indonesia…..…..……. 34
4.1.2. Peran Kementerian Komunikasi dan Informatika... 41
4.1.2.1. Direktorat Keamanan Informasi.....……. 43
4.1.2.2. Direktorat Komunikasi Publik…….…..…. 45
4.1.3. Peran Kementerian Pertahanan…… 47
4.1.3.1. Pusat Data dan Informasi……... 49
4.1.3.2. Pusat Komunikasi Publik…… 51
4.2. Analisis Data dan Hasil Temuan……... 54
4.2.1. Analisis Interpretasi naratif (*Narrative Interpretative Analysis)*……..…….. 54
4.2.2. Permasalahan Pola Keterbukaan Informasi bidang Pertahanan…….. 55
4.2.3. Pemecahan Masalah dalam Pola Keterbukaan Informasi bidang Pertahanan…… 60
4.2.3.1.Sistem Keamanan Informasi Pertahanan yang Diterapkan oleh Kementerian Komunikasi dan Informatika…… 61
4.2.3.2.Sistem Keamanan Informasi Pertahanan yang Diterapkan oleh Kementerian Pertahanan …….. 65
4.3. Pembahasan…… 68
4.3.1. Aspek Tindakan dalam Keunggulan Informasi….. 68

4.3.2. Aspek Perilaku dalam Partisipasi Masyarakat….. 71

5 SIMPULAN DAN SARAN 74

5.1. Simpulan 74

5.2. Saran 76

DAFTAR REFERENSI …….. 79

DAFTAR GAMBAR

Gambar 2.1. Kerangka Pemikiran……. 24
Gambar 4.1. Pola Keterbukaan Informasi Pertahanan 35
Gambar 4.2. Struktur Organisasi Kementerian Komunikasi dan Informatika ……..... 42
Gambar 4.3. Skema Kerja Direktorat Keamanan Informasi..... 44
Gambar 4.4. Skema Kerja Direktorat Komunikasi Publik…..... 46
Gambar 4.5. Struktur Organisasi Kementerian Pertahanan… 48
Gambar 4.6. Struktur Organisasi Pusat Data dan Informasi… 50
Gambar 4.7. Struktur Organisasi Pusat Komunikasi Publik… 54
Gambar 4.8. Statistik Data Serangan ke Situs Institusi Pemerintah……... 56
Gambar 4.9. Skema Indeks Keamanan Informasi (Indeks KAMI)……..... 64

DAFTAR LAMPIRAN

Lampiran 1. Daftar Narasumber……..... 83
Lampiran 2. Petunjuk Umum Wawancara……... 84
Lampiran 3. Surat Izin Penelitian…….. 87
Lampiran 4. Daftar Informasi Pertahanan di Lingkungan
Kementerian Pertahanan…….. 88
Lampiran 5. Daftar Informasi Pertahanan yang Dikecualikan
di Lingkungan Kementerian Pertahanan……. 103

DAFTAR SINGKATAN

ALUTSISHAN	:	Alat Utama Sistem Pertahanan
BAIS	:	Badan Intelijen Strategis
KAMI	:	Keamanan Informasi
KEMENHAN	:	Kementerian Pertahanan
KIP	:	Komisi Informasi Pusat
KOMINFO	:	Kementerian Komunikasi dan Informatika
KUATHAN	:	Kekuatan Pertahanan
LEMSANEG	:	Lembaga Sandi Negara
MABES TNI	:	Markas Besar Tentara Nasional Indonesia
NKRI	:	Negara Kesatuan Republik Indonesia
PASPAMPRES	:	Pasukan Pengaman Presiden
POTHAN	:	Potensi Pertahanan
RANAHAN	:	Sarana Pertahanan
RENHAN	:	Perencanaan Pertahanan
SISFOHANNEG	:	Sistem Informasi Pertahanan Negara
SMKI	:	Sistem Manajemen Keamanan Infomasi
STRAHAN	:	Strategi Pertahanan
TNI	:	Tentara Nasional Indonesia
UU	:	Undang-Undang

BAB 1

PENDAHULUAN

1.1. Latar Belakang

Globalisasi merupakan salah satu fenomena yang paling banyak memberikan pengaruh dalam dinamika kehidupan berbangsa dan bernegara saat ini, tidak terkecuali dalam bidang pertahanan. Penjagaan kedaulatan yang merupakan tugas utama setiap komponen di sektor pertahanan diartikan sebagai cakupan pemerintahan suatu negara yang memiliki pengaruh eksternal dan internal untuk wilayah tersebut.[1] Sifat dari kedaulatan tersebut dianggap sangat kontradiksi dengan sifat yang dibawa oleh perkembangan teknologi karena pengaruh besar teknologi terutama di bidang informasi dan komunikasi membuat adanya pengaburan batas-batas yang sebelumnya didefinisikan oleh kedaulatan sebuah negara-bangsa.[2] Beberapa futurolog dan teknolog bahkan melihat perkembangan teknologi informasi dan komunikasi telah menggerogoti otoritas dan kekuasaan negara[3] yang berdampak pada postur komponen pertahanan yang menjadi tumpuan dalam menghadapi ancaman-ancaman nontradisional di bidang keamanan.

Secara khusus dalam kajian peperangan, perkembangan teknologi di bidang informasi dan komunikasi telah mengubah paradigma perang dan mengantarkan pada generasi perang baru. Pada generasi perang kesatu hingga ketiga dikenal sifat perang yang berupa paradigma peperangan

[1] G. Evans dan J. Newnham, *Dictionary of International Relations,* Penguin Books, London, 1998, hal.504.

[2] A. Octavian, *Militer dan Globalisasi,* kata pengantar oleh I. G. Sujatmiko, UI Publishers, Jakarta, 2012, hal. 8.

[3] C.P.F. Luhulima, 'Kemajuan Teknologi Informasi dan Komunikasi: Saran untuk Strategi Keamanan Nasional', dalam Bantarto Bandoro (ed.), *Perspektif Baru Keamanan Nasional*, Percetakan Kanisius, Yogyakarta, 2006, hal.138.

simetris.[4] Pada perang generasi selanjutnya terutama sejak berakhirnya era perang dingin, terjadi evolusi besar dalam paradigma peperangan dalam konstelasi internasional. Derasnya arus globalisasi yang mengakibatkan perkembangan teknologi dalam bidang komunikasi dan informasi menjadi salah satu alasan terjadinya evolusi paradigma tersebut. Pada generasi terbaru yaitu generasi kelima, paradigma peperangan lebih dikenal sebagai peperangan asimetris.[5,6] Indonesia sebagai salah satu negara yang sedang melakukan perkembangan di berbagai bidang dituntut untuk siap dalam menghadapi perang generasi terbaru tersebut dan menyiapkan pertahanan dari ancaman-ancaman yang bersifat nontradisional khususnya dalam bidang teknologi informasi dan komunikasi.

Globalisasi selain membawa nilai pengembangan teknologi dan informasi yang sangat pesat juga mendorong berkembangnya paham demokrasi di berbagai negara. Keberadaan demokrasi dituntut untuk selalu ada dan menjadi pedoman seiring dengan kebijakan dan strategi yang diusung oleh pemerintahan suatu negara. Tidak terkecuali di Indonesia, keberadaan demokrasi menjustifikasi keinginan masyarakat untuk terciptanya sebuah keterbukaan informasi. Keterbukaan informasi tersebut memang sangat penting untuk kemajuan demokrasi dalam kehidupan berbangsa dan bernegara. Adanya keterbukaan informasi tersebut menyebabkan berbagai informasi yang dibutuhkan oleh publik sampai kepada publik secara

[4] Peperangan Simetris dimengerti sebagai peperangan yang melibatkan pihak yang serupa. Meski memliki perbedaan dalam beberapa sisi, tetapi secara umum kesetaraan antara kedua pihak tersebut dapat terlihat. Lihat R. Thornton, *Asymmetric Warfare*, Polity Press, Cambridge, 2007, hal. 4.

[5] Peperangan Asimetris dimengerti sebagai pilihan strategi yang dipilih oleh pihak yang dianggap lemah melawan pihak yang 'lebih kuat' dengan menggunakan senjata alternatif yang bersifat nonkonvensional dan tidak simetris sehingga dapat mengancam kerentanan pihak yang lebih kuat karena berpengaruh luas pada masyarakat sipil. Lihat 'Security Priorities in a Changing World', dalam *Strategic Defence Review,* HMSO, London, 1998, bab 2.

[6] Peperangan Asimetris memiliki pengertian lain yaitu, aksi kekerasan yang dilakukan oleh pihak yang 'lebih lemah' terhadap pihak yang 'lebih kuat'. Namun, dalam aksi tersebut pihak yang 'lebih lemah'memiliki pengaruh yang besar dalam sebagian besar level peperangan baik taktis maupun strategis dengan memanfaatkan keuntungan relatifnya melawan kerentanan yang dimiliki pihak yang 'lebih kuat'. Lihat, R. Thornton, hal. 1.

menyeluruh dan dapat diakses secara cepat. Meski di lain sisi, informasi vital dan kritis yang terkadang tidak perlu diketahui publik pun diketahui oleh publik terutama didukung dengan adanya Undang-Undang (UU) No. 14 tahun 2008 tentang Keterbukaan Informasi Publik.

Informasi publik didefinisikan oleh Kementerian Komunikasi dan Informatika Republik Indonesia sebagai informasi yang dihasilkan, disimpan, dikelola, dikirim, dan/atau diterima oleh suatu badan publik yang berkaitan dengan penyelenggara dan penyelenggaraan negara dan/atau penyelenggara dan penyelenggaraan badan publik lainnya yang sesuai dengan UU ini serta informasi lain yang berkaitan dengan kepentingan publik.[7] Salah satu jenis informasi publik yang harus diakomodasi oleh institusi publik adalah informasi bidang pertahanan. Informasi bidang pertahanan memiliki pengertian yang berbeda dengan informasi publik. Dalam beberapa literatur yang dikeluarkan oleh pemerintah Amerika Serikat, informasi pertahanan didefinisikan sebagai informasi yang dilindungi oleh pemerintah. Baik jika informasi tersebut merupakan informasi milik pemerintah dan dianggap rahasia atau informasi yang dimasukkan dalam klasifikasi normal.[8] Sedangkan menurut Kementerian Pertahanan Indonesia melalui KEP/880/ M / X / 2012 tanggal 25 Oktober 2012 tentang Tata Cara Penyebarluasan Informasi Pertahanan di Lingkungan Kementerian Pertahanan, informasi bidang pertahanan adalah informasi pertahanan yang dihasilkan, disimpan, dikelola, dikirim dan diterima oleh Kementerian Pertahanan yang berkaitan dengan penyelenggaraan sebagian urusan pemerintahan di bidang pertahanan. Sistem yang melingkupi informasi pertahanan tersebut dinamakan sistem informasi pertahanan negara yang merupakan integrasi data internal dan eksternal dalam jaringan komunikasi data yang terdiri dari data internal Kementerian Pertahanan yang terdiri dari

[7] Sekretariat Komisi Informasi Pusat, *Undang-Undang Republik Indonesia Nomor 14 Tahun 2008,* 2010, hal.5.

[8] J. K. Elsea, *CRS Report for Congress: Protection of National Security Information*, 2006, hal.4

informasi dari direktorat strategi pertahanan (Strahan) perencanaan pertahanan (Renhan), kekuatan pertahanan (Kuathan), potensi pertahanan (Pothan), dan sarana pertahanan (Ranahan) serta terintegrasi pula dengan data eksternal yang berasal dari ketiga angkatan militer yaitu Angkatan Darat, Angkatan Laut dan Angkatan Udara.[9]

Berkembangnya ruang siber pada era peperangan informasi saat ini mulai menjadi perhatian yang dianggap menyangkut pada kepentingan nasional. Hal ini pula yang memberi dampak besar pada perlakuan sebuah negara pada informasi, baik pada informasi publik serta informasi yang dirahasiakan. Dilihat dari Buku Putih Pertahanan Indonesia tahun 2008[10], dinyatakan bahwa Indonesia melakukan kegiatan pertahanan untuk mengawal kepentingan nasional Indonesia yaitu: kedaulatan Negara Kesatuan Republik Indonesia (NKRI), keutuhan wilayah Indonesia yang bersifat kepulauan dan keselamatan segenap bangsa dari segala bentuk ancaman terhadap Indonesia. Meskipun dalam implementasinya ruang siber merupakan ruang yang tidak mendasarkan pada kerangka pikir teritorial, tetapi terdapat relevansi dari kepentingan nasional tersebut dengan perlunya Indonesia memiliki doktrin dan strategi yang tepat dalam melindungi informasi bidang pertahanan Indonesia agar tidak berakibat pada hancurnya kepentingan nasional Indonesia.

Fenomena informasi sebagai sebuah ancaman nontradisional telah menimbulkan dampak yang luas dan memiliki variasi dari yang memiliki dampak lokal kedaerahan, nasional, hingga yang memiliki dampak internasional. Beberapa ancaman di level internasional yang pernah muncul, menurut Singer dan Friedman (2014)[11], dimulai dari keputusan Pemerintah

---

[9] H. Asrin, 'Sistem Informasi Pertahanan Negara Yang Terintegrasi Dalam Menghadapi Perang Informasi'*, Kementerian Pertahanan Republik Indonesia,* 21 Mei 2012, <http://www.kemhan.go.id/kemhan/?pg=73&id=204>*,* diakses pada 6 September 2014.

[10] Kementerian Pertahanan Republik Indonesia, *Buku Putih Pertahanan Indonesia 2008*, Kementerian Pertahanan Republik Indonesia, 2008, hal. 39.

[11] Lebih lanjut lihat di P.W Singer dan A. Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, New York, 2014, hal. 9.

Republik Rakyat Tiongkok yang melancarkan serangan siber mutakhir pada perusahaan Google dan beberapa perusahaan Amerika Serikat lainnya, bocornya banyak arsip penting digital dengan tingkat kerahasiaan tinggi milik banyak negara oleh sebuah situs bernama WikiLeaks, hingga revolusi kebangkitan dunia Arab dengan kecepatan, kekuatan dan efek mobilisasi yang sangat luas dengan campur tangan teknologi di dalamnya.

Pada level nasional di Indonesia, keterbukaan informasi pertahanan justru banyak dimanfaatkan oleh Lembaga Swadaya Masyarakat untuk mengontrol institusi publik, dan digunakan oleh media untuk mengetahui hal-hal yang tidak sepatutnya diketahui. Salah satu bentuknya adalah informasi mengenai persenjataan apa saja yang dimiliki dan digunakan Indonesia sebagai alat utama sistem pertahanan (alutsishan) menjadi pembicaraan hangat masyarakat awam Indonesia dan dijadikan komoditas dalam percaturan politik Indonesia. Dampak dari topik yang tersebar di masyarakat tersebut adalah terbaginya masyarakat menjadi pihak yang pro dan kontra, meskipun dalam substansinya banyak masyarakat yang tidak mengerti mengenainya. Mudahnya informasi ini didapatkan oleh masyarakat menimbulkan pertanyaan apakah hal tersebut merupakan hal yang wajar sebagai akibat dari demokrasi dan luasnya perkembangan teknologi, atau hal ini adalah sebuah fenomena yang dapat membahayakan kepentingan nasional dalam jangka panjang. Jika memang hal tersebut adalah hal yang wajar, bagaimana sebuah negara dapat memastikan dampak tersebut tidak sampai membahayakan kepentingan nasional Indonesia.

Meskipun peneliti percaya bahwa demokrasi dan perkembangan teknologi yang berjalan secara selaras tidak selalu bernilai negatif sepenuhnya bagi bangsa Indonesia. Namun, dalam menghadapi era yang menuntut pemahaman akan teknologi informasi dan komunikasi yang tinggi, Indonesia sebagai negara yang kuat harus dapat menemukan pola keterbukaan informasi yang tepat sehingga dapat menunjang posisi

Indonesia dalam konstelasi politik internasional. Terlebih lagi jika pola tersebut berkaitan dengan informasi vital dalam bidang pertahanan.

Sebagaimana uraian permasalahan di atas maka peneliti mengangkat tesis yang berjudul:

Pola Keterbukaan Informasi Bidang Pertahanan di Indonesia sebagai Ancaman Nontradisional

1.2. Rumusan Masalah

Pada bagian latar belakang yang telah diuraikan dapat diketahui bahwa strategi dan pola menghadapi peperangan informasi di Indonesia belum dilakukan secara komprehensif dengan menerapkan kebijakan yang tepat. Negara Republik Indonesia sebagai negara demokrasi memperkenankan partisipasi dari warga negaranya terhadap sistem pemerintahan, termasuk bidang pertahanan. Namun, sifat peperangan informasi yang sangat dinamis menimbulkan tantangan yang konstan sebagai sebuah ancaman nontradisional bagi sebuah negara. Pola keterbukaan dan pola keamanan informasi pertahanan yang tidak berjalan secara selaras dan tepat dapat menimbulkan kerugian bagi kepentingan nasional Indonesia. Dalam menghindari hal tersebut diperlukan pola keterbukaan informasi bidang pertahanan yang lebih baik dan dapat bekerja secara maksimal melindungi kepentingan nasional Indonesia. Pola yang dibutuhkan Indonesia saat ini adalah mekanisme atas keterbukaan informasi pertahanan yang tepat sehingga dapat memenuhi nilai partisipasi masyarakat untuk mengetahui informasi pertahanan yang diperkenankan namun tetap memenuhi nilai keamanan dari informasi pertahanan yang pada tujuan akhir dapat memberikan keunggulan informasi atas pemerintah Indonesia.

Berdasarkan rumusan masalah tersebut maka pertanyaan penelitian yang akan diangkat dalam tesis ini yaitu,

1. Bagaimana pola keterbukaan informasi bidang pertahanan yang dimiliki Indonesia?
2. Bagaimana penerapan pola keterbukaan informasi pertahanan agar dapat secara maksimal menghadapi ancaman nontradisional?

1.3. Tujuan dan Signifikansi Penelitian

Merujuk dari rumusan masalah tersebut, tujuan dari penelitian ini adalah sebagai berikut:

1.3.1. Untuk menganalisis dan meninjau struktur, sistem, tindakan dan perilaku terhadap informasi bidang pertahanan Indonesia dan dampaknya pada posisi Indonesia dalam peperangan informasi.

1.3.2. Untuk memberikan saran dan masukan serta dapat menemukan sistem dan tata cara informasi bidang pertahanan yang tepat bagi Indonesia sehingga dapat mewadahi partisipasi masyarakat sekaligus melindungi keunggulan informasi Indonesia dalam menghadapi ancaman nontradisional.

1.4. Manfaat Penelitian

Penelitian atau pembahasan suatu masalah dalam penelitian ini diharapkan dapat memberikan manfaat dan berguna bagi pihak-pihak yang tertarik dan berkepentingan sebagaimana permasalahan yang diangkat dalam penelitian ini. Adapun kegunaan dari penelitian ini meliputi dua bagian, yaitu:

1.4.1. Secara Teoritis, diharapkan penelitian ini dapat :

a. Memberikan manfaat bagi perkembangan ilmu pengetahuan baik dalam bidang sosial, politik, serta kajian-kajian tentang pertahanan keamanan.

b. Menambah bahan kepustakaan atau tambahan referensi bagi kepentingan yang bersifat akademis berkaitan dengan penanganan peperangan informasi dan siber khususnya di Indonesia.

1.4.2. Secara praktis, diharapkan penelitian ini dapat:

Hasil penelitian ini diharapkan dapat memberikan manfaat dan tolak ukur bagi semua pihak yang secara langsung terjun dalam pembuatan dan penerapan kebijakan serta strategi yang berhubungan dengan keterbukaan informasi bidang pertahanan dan keamanan, sehingga Indonesia dapat mencapai tujuan nasionalnya dalam peperangan informasi saat ini.

1.5. Ruang Lingkup dan Gambaran Desain Penelitian

1.5.1. Ruang Lingkup

Penelitian ini dijadwalkan dilaksanakan pada Agustus 2014 hingga Januari 2015 serta mengambil lokasi penelitian di wilayah Jakarta dan Bogor sehingga penelitian ini diharapkan mampu menghasilkan analisis yang mendalam dan komprehensif sebagaimana tujuan dan manfaat yang ingin dicapai dalam penelitian ini melalui analisis jangka pendek dan jangka panjang.

1.5.2. Gambaran Desain Penelitian

Dalam penelitian ini, peneliti akan mendesain penulisan menjadi lima bab sebagai berikut:

BAB 1 PENDAHULUAN

Bab ini berisi mengenai gambaran yang bersifat umum dan menyeluruh secara sistematis, yang terdiri dari latar belakang masalah, identifikasi masalah, maksud dan tujuan penelitian, kegunaan penelitian, kerangka pemikiran, ruang lingkup dan desain penelitian, serta sistematika penulisan.

BAB 2 TINJAUAN PUSTAKA, KERANGKA PEMIKIRAN, DAN PENELITIAN YANG RELEVAN

Bab ini membahas mengenai teori, definisi, asas, doktrin, dan kepustakaan lainnya yang memiliki keterkaitan dengan permasalahan yang diangkat. Selain itu dalam bab ini juga dibahas mengenai kerangka pikir penelitian serta penelitian-penelitian lain yang memiliki relevansi dengan permasalahan yang diangkat.

BAB 3 METODE PENELITIAN

Bab ini membahas metode penelitian, meliputi;

1) Sumber data baik primer maupun sekunder,
2) Desain penelitian yang meliputi teknik pengumpulan data melalui observasi, wawancara mendalam, dan studi literatur atau dokumentasi terhadap subyek dan obyek penelitian.
3) Teknik analisis data melalui tahapan reduksi data, kategorisasi, sintesisasi dan menyusun preposisi penelitian. Pada akhir bab ini akan dijelaskan prosedur penelitian terkait dengan rencana waktu dan tempat penelitian.

BAB 4 ANALISIS INFORMASI BIDANG PERTAHANAN DI INDONESIA DALAM MENGHADAPI ANCAMAN NONTRADISIONAL

Bab ini menganalisis mengenai sistem informasi bidang pertahanan Indonesia dan dampaknya terhadap posisi Indonesia dalam peperangan informasi. Melalui analisis tersebut diharapkan dapat diketahui desain ideal dari keterbukaan sistem informasi bidang pertahanan di Indonesia.

BAB 5 SIMPULAN DAN SARAN

Bab ini merupakan bagian akhir yang menguraikan simpulan dari penelitian yang telah dikemukakan dalam bab-bab sebelumnya, serta saran yang

diberikan oleh Peneliti guna mencapai kemajuan dalam hal menghadapi peperangan informasi, khususnya di Indonesia.

BAB 2

TINJAUAN PUSTAKA, KERANGKA PEMIKIRAN, DAN PENELITIAN RELEVAN

2.1. Tinjauan Pustaka

Fenomena informasi sebagai sebuah ancaman nontradisional telah menimbulkan dampak yang luas dan memiliki variasi dari yang memiliki dampak lokal kedaerahan, nasional, hingga yang memiliki dampak internasional. Beberapa contoh tersebut adalah pada Republik Rakyat Tiongkok yang melancarkan serangan siber mutakhir pada perusahaan Google dan beberapa perusahaan Amerika Serikat lainnya, bocornya banyak arsip penting digital dengan tingkat kerahasiaan tinggi milik banyak negara oleh sebuah situs bernama WikiLeaks, hingga revolusi kebangkitan dunia Arab dengan kecepatan, kekuatan dan efek mobilisasi yang sangat luas dengan campur tangan teknologi di dalamnya. Contoh lain yang dianggap pula sebagai salah satu hasil dari peperangan informasi yang pernah terjadi adalah kejadian di Estonia. Kejadian yang terjadi pada tahun 2007 tersebut dilakukan terhadap pemerintah Estonia yang berdampak pada gangguan akses secara besar-besaran pada level nasional. Estonia merupakan negara di Uni Eropa yang memiliki tingkat konektivitas tertinggi. Mayoritas dari warga negara Estonia melakukan kegiatannya, dari kegiatan perbankan hingga pemilihan umum melalui jaringan internet. Adanya ketergantungan yang besar terhadap sistem informasi membuat sistem ekonomi dan pemerintahan di Estonia lumpuh dalam waktu yang singkat.[12] Menteri Luar Negeri Estonia saat itu, Urmas Paet, menyatakan bahwa kejadian tersebut merupakan

[12] R. A. Clarke dan R. K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It,* HarperCollins, New York, 2010, hal. 13.

serangan yang virtual, psikologis, namun nyata.[13] Dengan adanya kejadian itu, Estonia mengatur kembali pola yang diimplementasikannya untuk menghadapi peperangan informasi sebagai ancaman nontradisional. Melihat begitu pentingnya menentukan pola dalam menghadapi ancaman nontradisional, maka dalam penyusunan tesis ini peneliti memasukkan beberapa teori yang terkait. Untuk menunjang penelitian ini, peneliti menggunakan teori, konsep, maupun definisi yang memiliki relevansi dengan penelitian. Teori, konsep, dan definisi-definsi akan digunakan untuk mendukung analisis permasalahan yang diangkat dalam penelitian ini.

2.1.1. Pola

Pola diartikan dalam bahasa Indonesia sebagai sistem atau cara kerja dalam sebuah pemerintahan.[14] Diartikan dari bahasa Inggrisnya yakni dari kata *pattern* yang berarti sebuah struktur persepsi, sebuah cara operasional yang dibentuk dari serangkaian tindakan dan perilaku, atau sesuatu yang digunakan sebagai sebuah petunjuk atau pedoman dalam melakuan sesuatu yang lain.[15] Dalam pengembangan konsep teoritisnya, pola diambil dari pendekatan teori matematis milik Ulf Grenader[16] yang mencakup pengertian sebuah formulasi yang didistribusikan dari variabel-variabel dan model-model yang diobservasi dan menimbulkan sebuah sintesis tertentu dari variabel dan model tersebut, tidak hanya sebuah analisis. Dari beberapa pendapat tersebut mengenai pola, dapat ditemukan bahwa pola merupakan sebuah konsep yang berkaitan dengan struktur, sistem, atau serangkaian tindakan dan perilaku yang menghasilkan sebuah sintesis yakni petunjuk atau pedoman yang digunakan untuk mengatur suatu hal yang lain. Dengan adanya pola, dapat ditentukan solusi dari permasalahan yang dihadapi pemerintahan.

---

[13] Singer dan Friedman, hal. 110.
[14] Kamus Besar Bahasa Indonesia dalam jaringan diakses dari www.kbbi.web.id
[15] Definisi *Pattern* diakses dari www.wolframalpha.com
[16] U. Grenader, *General Pattern Theory,*Oxford Science Publications,Oxford, 1994.

2.1.2. Teori Informasi

Pada akhir abad keduapuluh, peran informasi dan komunikasi elektronik semakin besar. Dapat dilihat bahwa revolusi transmisi data telah membawa manfaat yang sangat banyak. Karena hal tersebut pula masyarakat memiliki kemampuan baru untuk memperoleh informasi akurat dan terverifikasi melalui teknologi siber secara mudah dan berkembang hingga pada jumlah yang tidak berbatas. Akibat peran yang semakin luas tersebut, akhirnya banyak muncul definisi mengenai teori informasi pada tulisan yang dipublikasi pada akhir abad keduapuluh. Salah satunya adalah menurut Edward Waltz yang menyatakan informasi sebagai sebuah esensi dan manifestasi persaingan, konflik dan peperangan. Informasi menurut Waltz dibedakan menjadi tiga sesuai dengan isi dan proses yang dilaluinya[17], yaitu:

1. Data: Pengamatan individu, pengukuran, pesan jenis lama yang merupakan bentuk dari level informasi paling rendah. Dapat juga diartikan sebagai komunikasi antarmanusia, pesan teks, pesan apapun yang melewati media elektronik dan segala instrumen ilmiah yang fenomena utamanya adalah sumber utama dari sebuah data.
2. Informasi: Serangkaian data yang terorganisasi disebut sebagai informasi. Proses pengorganisasian sering mencakup, pemilahan, klasifikasi, pengindeksan dan menghubungkan data untuk menempatkan elemen data dalam konteks relasional dalam rangka melakukan analisis dan pencarian berikutnya.
3. Pengetahuan: Sekumpulan informasi yang telah dianalisis dan dipahami merupakan pengetahuan. Pemahaman terhadap informasi memberikan tingkat pemahaman secara komprehensif baik secara statis maupun dinamis akan hubungan obyek-obyek

[17] E. Waltz, *Information Warfare Principles and Operations,* Artech House, London, 1998, hal.1-2.

data dan pemahaman pola akan perilaku obyek tersebut di masa lampau, saat ini, maupun di masa mendatang. Dalam konteks militer, pengertian tersebut seringkali disebut sebagai intelijen.

Pengertian yang dipaparkan sebagaimana di atas adalah pengertian dari abad keduapuluh. Meskipun definisi informasi secara akademis baru ada pada abad keduapuluh, Sun Tzu dalam bukunya yang tersebar sejak abad ke 6 sebelum masehi telah memandang pentingnya informasi melalui tulisannya dalam *Art of War* tentang informasi[18], sebagai berikut;

1. Informasi adalah bentuk dari intelijen dan kemampuan untuk meramalkan kemungkinan yang terjadi di masa depan dan pihak yang memiliki kemampuan tersebut adalah pihak yang akan memenangkan peperangan. Dalam tulisan aslinya, Sun Tzu menulis,

   "Thus, what enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge"

2. Kemampuan untuk mengontrol informasi yang dikomunikasikan oleh lawan, baik dengan muslihat, pendadakan, maupun penyangkalan adalah sebuah kontribusi yang dapat membingungkan persepsi lawan.

   "All warfare is based on deception [of the enemy]," and, "O divine art of subtlety and secrecy! Through you we learn to be invisible, through you inaudible."

3. Pemenang perang yang sebenarnya adalah yang dapat menggunakan informasi untuk mempengaruhi persepsi lawan sehingga memilih untuk mengurangi keinginan berperangnya dibanding menggunakan kekuatan militer.

   "In the practical art of war, the best thing is to take the enemy's

[18] Dikumpulkan dari buku karya Sun Tzu, *Art of War*, Shambala, Boston, 1988.

country whole and intact....Hence to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting."

2.1.2.1. Keterbukaan Informasi

Keterbukaan informasi menurut UU Republik Indonesia nomor 14 tahun 2008 merupakan hak untuk memperoleh informasi sebagai sarana dalam memaksimalkan pengawasan publik terhadap penyelenggaraan negara dan badan publik lainnya dan segala sesuatu yang berakibat pada kepentingan publik. Keterbukaan informasi publik merupakan salah satu ciri penting negara demokratis yang menjunjung tinggi kedaulatan rakyat untuk mewujudkan penyelenggaraan negara yang baik.[19] Dalam konteks bidang keamanan dan pertahanan, negara demokratis membuka ruang-ruang tersedianya informasi yang dapat diakses masyarakat dengan tujuan agar hak-hak warga negara tetap terjaga dan dapat dipenuhi secara baik oleh negara. Di samping itu, adanya keterbukaan informasi dalam sistem sebuah negara juga dapat menjadikan aktor pertahanan lebih profesional dengan bekerja dilandasi sesuai hukum yang berlaku.

Pada tujuan yang lebih luas, diharapkan keterbukaan informasi dapat mengantarkan pada, (1) Publik yang lebih banyak mendapat informasi dapat berpartisipasi lebih baik dalam proses demokrasi; (2) Parlemen, pers dan publik harus dapat dengan wajar mengikuti dan meneliti tindakan- tindakan yang diambil pemerintah; (3) Pegawai pemerintahan mengambil keputusan-keputusan penting yang berdampak pada kepentingan publik; dan agar bertanggung jawab pemerintah harus menyediakan informasi yang lengkap mengenai apa yang dikerjakan; (4) Arus informasi yang lebih baik sehingga dapat menghasilkan pemerintahan yang efektif dan membantu pengembangan yang lebih fleksibel; (5) Kerjasama antara publik dan

[19] Kementerian Komunikasi dan Informatika Republik Indonesia, *Undang-Undang Republik Indonesia No.14 Tahun 2008 tentang Keterbukaan Informasi Publik*, Kementerian Komunikasi dan Informatika Republik Indonesia, 2013, hal. 1.

pemerintah akan semakin erat karena informasi yang tersedia semakin banyak.

2.1.2.2. Resiko Ancaman pada Sistem Informasi

Kontrol keamanan yang efektif untuk sebuah sistem informasi didasari dari identifikasi resiko keamanan yang mungkin terjadi pada sebuah sistem informasi. Keamanan informasi tersebut adalah sebuah cabang dalam teknologi informasi yang mengkhususkan perhatian pada metode dan teknik untuk melindungi informasi dan sistem informasi dari akses, penggunaan, penyebaran, perusakan, perubahan, dan penghancuran tanpa otorisasi yang sah. Dalam hal ini Kementerian Komunikasi dan Informatika Republik Indonesia sebagai pihak yang melakukan kegiatan pengamanan informasi di Indonesia, mengidentifikasikan beberapa resiko ancaman yang mungkin terjadi pada sebuah sistem informasi suatu institusi, yaitu[20];

(a) *Error* atau kesalahan data yang meliputi kesalahan dalam pemasukan data, kesalahan pemrosesan data dalam sistem informasi yang disebabkan *bug* ataupun kesalahan konfigurasi sistem. Ancaman ini sebagian besar datang dari kesalahan yang dilakukan oleh aspek manusia atau *human error.*

(b) Penipuan dan pencurian data yang dapat dilakukan oleh pihak internal yang ingin memanfaatkannya untuk kepentingan pribadinya, atau penyusup dari luar yang melakukan pencurian fisik terhadap perangkat komputer yang berisi data sensitif.

(c) Sabotase pegawai adalah ancaman yang dilakukan oleh pegawai yang tidak puas terhadap institusi maupun atasan sehingga melakukan usaha eksploitasi terhadap celah keamanan yang diketahuinya.

(d) Kegagalan dukungan infrastruktur juga menjadi ancaman dalam sistem informasi yang meliputi kegagalan aliran listrik, kerusakan saluran

[20] Kementerian Komunikasi dan Informatika, *Panduan Topologi dan Keamanan Sistem Informasi*, Kementerian Komunikasi dan Informatika, 2013, hal. 11-14.

komunikasi, banjir, *mogok* massal, dan sebagainya. Hal ini dianggap ancaman karena dapat menjadi *downtime* bagi institusi.

(e) Serangan *hacker* jahat didefinisikan sebagai ancaman dari pihak yang masuk ke dalam sistem tanpa izin. Ancaman ini dapat dilakukan oleh pihak internal maupun eksternal institusi. Kerusakan yang ditimbulkan oleh ancaman ini adalah kehilangan data sensitif dan rusaknya reputasi institusi, terutama dalam ranah perbankan.

(f) Espionasi industri terjadi saat data rahasia milik institusi komersial atau pemerintahan yang kemudian digunakan oleh institusi lain. Ancaman ini menjadi sangat berbahaya jika data yang diketahui adalah data milik negara.

(g) Program berbahaya juga dapat menjadi ancaman, terutama yang mengacu pada virus, worm, Trojan dan perangkat lunak asing lainnya yang dapat menghambat aktivitas operasional institusi tersebut.

(h) Pelanggaran privasi adalah ancaman yang dapat dilakukan oleh banyak pihak, seperti pemerintah, *hacker,* atau administrator dalam sebuah institusi. Ancaman pelanggaran privasi ini adalah aktivitas yang menyangkut penyebaran, penggunaan dan perubahan atas data pribadi seseorang tanpa otorisasi orang tersebut. Ancaman ini biasanya menjadi pintu masuk bagi ancaman-ancaman yang sebelumnya telah disebutkan.

2.1.2.3. Teori Keunggulan Informasi

Dalam tesis ini, peneliti menggunakan teori keunggulan informasi sebagai teori yang akan dapat menjelaskan pengamanan informasi sebagai salah satu usaha mencapai keunggulan informasi dan berperan untuk berjalan selaras dengan pola keterbukaan informasi pertahanan. Informasi saat ini tidak hanya sebagai data yang menyokong dan menentukan peperangan, pada perkembangannya, informasi telah menjadi sebuah laga peperangan atau *battlefield* yang disebut juga sebagai peperangan informasi.

Dalam laga peperangan informasi inilah, menurut Franklin D. Kramer[21], siber telah menjadi elemen dan di waktu yang sama menjadi pendukung untuk mendapatkan kekuasaan baik bagi negara, institusi, individu maupun entitas lainnya, bahkan untuk teroris dan kriminal.

Dorothy Denning menjelaskan bahwa, peperangan informasi adalah sebuah operasi yang menargetkan informasi melalui media komputer dalam rangka memenangkan beberapa keuntungan atau unggul atas lawan. Denning menuliskan bahwa,

"*Operations that target or exploit information media in order to win some advantage over an adversary. Its interpretation is so broad that it includes not just hacking but all of electronic warfare and all existing intelligence-gathering techniques, and propaganda too.*"[22]

Kajian peperangan asimetris juga meyakini bahwa di masa yang akan datang akan menggunakan konsep keunggulan informasi[23] lebih luas lagi, karena pasukan yang dimiliki oleh tiap negara tidak akan terbatas pada segmentasi ruang udara, laut dan darat tetapi juga memperluas akses yang dimilikinya hingga ke sistem informasi yang dimiliki oleh pemerintah. Tujuan dari operasi peperangan tersebut adalah keunggulan informasi yang didefinisikan oleh Kementerian Pertahanan Amerika Serikat sebagai kemampuan suatu institusi untuk mengumpulkan, memproses dan menyebarkan informasi tanpa gangguan dari pihak lawan sementara memanfaatkan kemampuan tersebut untuk menangkal gangguan aliran informasi dari lawan dengan menghalau pengumpulan, proses dan penyebaran informasi milik lawan.[24] Dalam jangka yang lebih panjang,

---

[21] F. D. Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework", dalam F. D. Kramer, S. Starr dan L. K. Wentz, eds., *Cyberpower and National Security*, Washington D.C., National Defense University Press, 2009.

[22] D. Denning, *Information Warfare and Security*, Addison-Weasley, Washington DC, 1999, hal. 11-12.

[23] H. Binnendijk dan R. L. Kugler, *"*Adapting Forces to a New Era: Ten Transforming Concepts", *Defense Horizon*, no.5, 2001, National Defense University, Washington DC, hal. 3.

[24] Joint Chiefs of Staff, *Joint Vision 2010*, U.S. Department of Defense, Washington D.C., July 1997, hal. 7.

keunggulan informasi dapat mengantarkan pihak musuh untuk dapat mendominasi peperangan sebagai alat untuk dapat mengendalikan peperangan, mengalahkan pasukan operasional musuh dan menghancurkan pasukan musuh melalui cara pendudukan wilayah kunci, dan menciptakan keuntungkan politik.

2.1.3. Konsep Ancaman Nontradisional

Dalam konsep keamanan tradisional diasumsikan bahwa sebuah sistem politik negara ditandai melalui keteraturan yang terjadi dalam wilayah domestik dan ketidakteraturan atau anarki yang datang dari aspek eksternal.[25] Sedangkan pada konsep pertahanan nasional, asumsi yang muncul dari konsep keamanan tradisional adalah, jika sebuah pemerintahan sebagai penentu dalam dinamika politik, diancam oleh kekuatan militer dari musuh asing maka warga negara di dalamnya juga dianggap terancam. Namun, menurut teori yang disampaikan oleh Joseph S. Nye dan David A. Welch, bahwa saat ini, aktor yang bermain dalam politik internasional dan saling melakukan interaksi jumlahnya sangat banyak dan dinamika dari konsep keamanan menjadi semakin kompleks.

Sebagai dampak perubahan dari konsep ancaman yang bersifat tradisional menjadi ancaman keamanan nontradisional, negara mengalami kesulitan dalam menghadapai isu-isu kompleks yang muncul sebagai ancaman peperangan jenis baru. Ancaman nontradisional secara spesifik didefinisikan sebagai kegiatan peperangan yang melibatkan sisi yang saling berlawanan dengan tidak terorganisasi secara jelas dan tidak selalu menggunakan senjata konvensional atau pasukan yang terstruktur.[26]

---

[25] K. Booth, 'Two Terrors, One Problem', dalam E. Aydinli dan J. N. Rosenau, eds., *Globalization, Security, and the Nation-State: Paradigms in Transition* , New York, University of New York, 2005.

[26] W. R. Schilling, 'Nontraditional Warfare Threats', dalam W. R. Schilling, ed., *Nontraditional Warfare: Twenty-First Century Threats and Responses,* Washington D.C, Brassey's Inc., 2002, hal. 4-8.

Beberapa jenis ancaman nontradisional yang dituliskan oleh William R. Schilling, seperti terorisme, penggunaan senjata pemusnah massal, dan termasuk peperangan informasi. Dalam menghadapi ancaman nontradisional, sebuah negara tidak efektif dalam penggunaan kekuatan konvensional tetapi harus membentuk kembali pola, taktik, organisasi, dan perilaku.

2.1.4. Teori Partisipasi Masyarakat

Teori partisipasi masyarakat yang diangkat dalam penelitian ini berusaha secara seimbang menggunakan teori partisipasi masyarakat tradisional seperti pemikiran Almond Verba (1978), menyatakan bahwa partisipasi masyarakat terutama dalam bidang politik adalah, serangkaian aksi legal yang dilakukan oleh masyarakat sipil yang secara kurang lebih bertujuan untuk mempengaruhi pemilihan personil dalam pemerintahan atau aksi yang akan mereka lakukan.

"By political participation we refer to those legal acts by private citizens that are more or less directly aimed at influencing the selection of governmental personnel and/or the actions that they take, broader efforts at mobilizing. From voting, donating money to advocacy groups, contacting local representatives, and reporting issues in a community, the assessment of the levels of actions (and their change over time) has been well documented."[27]

Dibandingkan teori tradisional mengenai partisipasi masyarakat, saat ini pengertian tersebut telah sedikit bergeser dengan munculnya variabel teknologi dalam sistem politik masyarakat. Pengertian yang dikemukakan Verba sedikit bergeser dengan berubahnya pula infrastruktur teknologi dan bagaimana masyarakat saling berkorespondensi yang berpengaruh pada cara masyarakat menilai sebuah pemerintahan yang baik.

"… *by being altered by shifting patterns of communication prompted by new digital technological infrastructures and their corresponding practices. Breaking down these actions to their correlated affective qualities, we look at*

[27] S. Verba, N. H. Nie , dan Jae-on Kim, *Participation and Political Equality: A Seven-Nation Comparison,* Cambridge University Press, Cambridge ,1978, hal. 134.

trust and empowerment as the basic building blocks of civic engagement, and demonstrate how technological mediation is necessitating"[28]

Menurut Terry F. Buss, F. Steven Redburn, dan Kristina Guo, dalam teori partisipasi masyarakat tersebut terdapat tujuan-tujuan yang ingin dicapai[29], yaitu;

(1) Membuat alam demokrasi semakin demokratis. Hal ini berarti bahwa masyarakat didorong untuk dapat melakukan *self-government*[30] melalui perluasan dan pendalaman keterlibatan masyarakat dalam pemerintahan . Dengan melakukan hal tersebut akan dapat diciptakan alam demokrasi yang lebih demokratis.
(2) Melakukan redefinisi terhadap struktur kekuatan politis. Hal ini ditandai dengan adanya partisipasi yang lebih besar dari masyarakat-masyarakat yang memiliki sumber kekuasaan lebih rendah seperti masyarakat berpendidikan rendah atau masyarakat yang tinggal di daerah pedalaman.
(3) Meningkatkan tingkat kredibilitas dan legitimasi dari masyarakat terhadap pemerintah. Saat suatu pemerintahan dinilai memiliki kredibilitas yang tinggi, maka akan timbul legitimasi yang besar dari warga negara untuk menjalamkan kebijakan dan program yang dimiliki pemerintahan.
(4) Menertibkan konflik dan membangun konsensus bersama. Pemerintahan yang demokratis terbangun ketika terbangun kesamaan visi, misi, dan tujuan dalam masyarakat. Partisipasi masyarakat diharapkan dapat menyelesaikan ketidaksepakatan

[28] E. Gordon, J. Baldwin-Philippi, dan M. Balestra, *Why We Engage: How Theories of Human Behavior Contribute to Our Understanding of Civic Engagement in a Digital Era,* Berkman Center at Harvard University, Cambridge, 2013, hal. 18.

[29] T. F. Buss, F. S. Redburn, dan K. Guo, 'An overview of the Issue', dalam T. F. Buss, F. S. Redburn, dan K. Guo (eds), *Modernizing Democracy: Innovations in Citizen Participation,* M.E Sharpe, New York, 2006, hal.9.

[30] *Self-government* berarti mewujudkan tatanan masyarakat yang madani tetapi tanpa terlalu banyak bergantung pada pemerintah dan sistem politik yang paternalistik. Lihat T. F. Buss, F. S. Redburn, dan K. Guo, hal.6.

dalam berbagai masalah dan terhindar dari konflik yang menggunakan kekerasan.

(5) Mendorong munculnya opini dan konsultasi dari masyarakat. Tujuan ini dianggap paling tidak kontroversial dibandingkan dengan tujuan-tujuan lainnya. Karena tujuan ini memberikan kesempatan pada masyarakat menyuarakan opininya tentang bagaimana suatu kebijakan harus dibuat, bagaimana kebijakan tersebut diterapkan, dan bagaimana kebijakan tersebut dapat ditingkatkan.

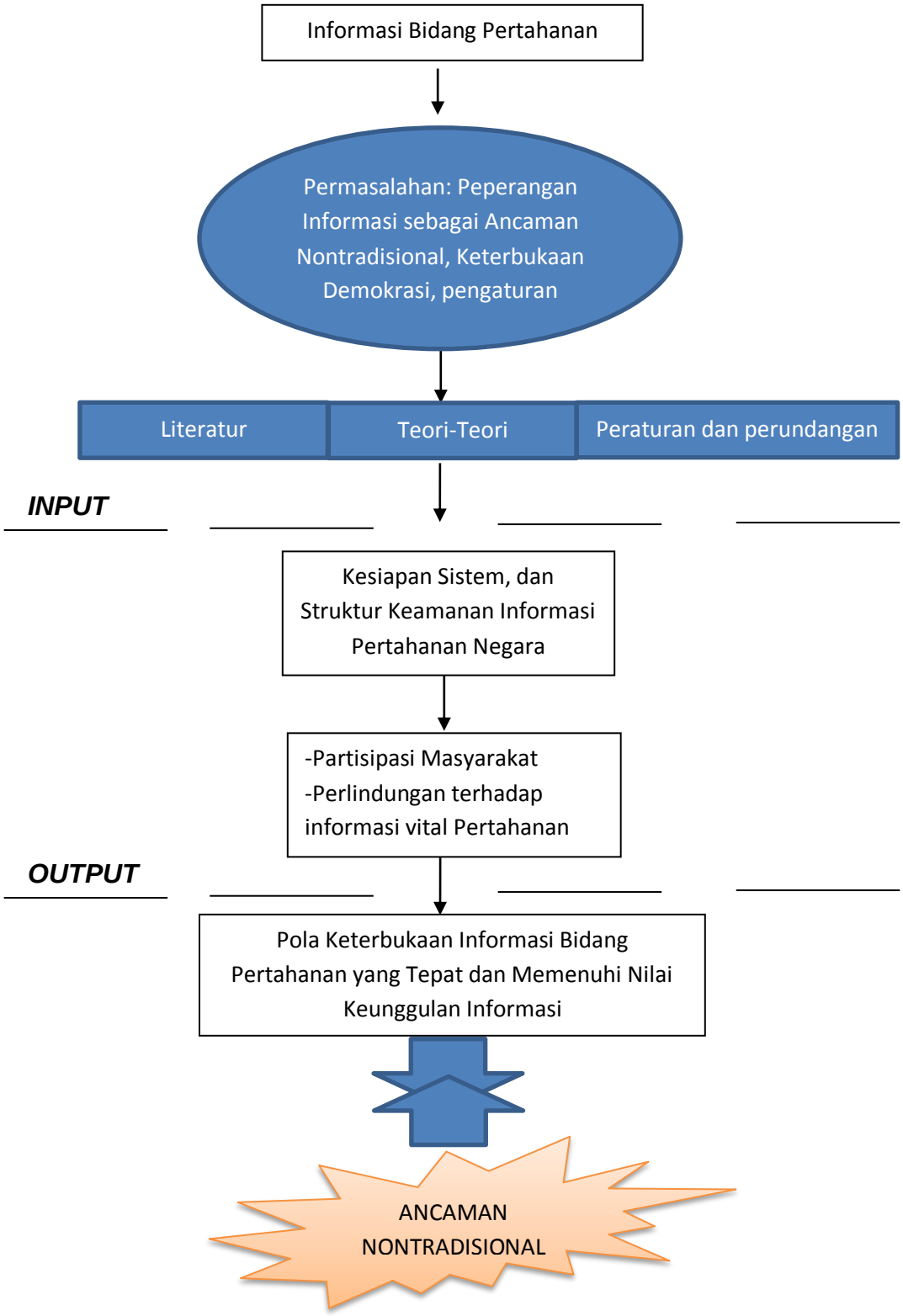
(6) Meningkatkan akuntabilitas dan transparansi dalam tingkat pemerintahan. Dengan adanya partisipasi masyarakat, akan lebih banyak keputusan yang diambil dengan masyarakat sebagai dasar pertimbangan kebijakan tersebut. Melalui hal tersebut maka nilai akuntabilitas aparat-aparat pemerintah semakin tinggi dan transparansi dapat dicapai.

2.2. Kerangka Pemikiran

Kerangka pikir dalam penelitan didasarkan pada rentannya keberadaan informasi pemerintah Indonesia di ranah dunia siber, terutama mengenai informasi vital bidang pertahanan. Dalam lingkungan regional dan global yang saat ini mendorong tersebar dengan cepatnya informasi terutama menggunakan perantara siber, setiap negara termasuk Indonesia didorong untuk memilki strategi dan doktrin baru yang dapat beradaptasi dengan keadaan tersebut. Melalui UU nomor 14 tahun 2008 yang dimiliki Indonesia saat ini mengharuskan setiap kementerian pemerintah untuk membuka informasi kepada publik dengan mengatur pula mengenai beberapa pengecualian. Hal ini memberikan dampak yang baik terutama dalam hal demokratisasi karena meningkatkan pengetahuan masyarakat akan apa yang dikerjakan oleh pemerintah. Di sisi lain juga memberikan tantangan dan ancaman terhadap pola keterbukaan informasi bidang pertahanan di

Indonesia. Meskipun, dalam tulisan ini nantinya akan meninjau pula mengenai penerapan UU tersebut terutama tentang informasi bidang pertahanan. Diharapkan melalui tinjauan tersebut dapat diwujudkan kesiapan yang lebih matang dari Kementerian Pertahanan Indonesia dalam menghadapi peperangan informasi.

Adapun untuk mencapai hasil penelitian yang mendalam dan komprehensif peneliti mencoba menganalisis dua komponen utama yang akan menjadi perhatian peneliti yaitu terjaminnya partisipasi masyarakat untuk mengetahui tentang informasi pertahanan namun di sisi lain tetap menjaga keamanan informasi bidang pertahanan sehingga tidak digunakan sebagai senjata oleh pihak lawan. Adapun preposisi dalam penelitian ini adalah kecermatan dari *stakeholders* yang berperan dalam penerapan kebijakan keterbukaan informasi bidang pertahanan ini sehingga dapat tetap memilki keunggulan informasi terhadap lawan di dalam peperangan informasi saat ini.



Gambar 2.1. Kerangka Pemikiran

2.3. Hasil Penelitian yang Relevan

Dalam menulis tesis ini, peneliti menemukan telah terdapat beberapa penelitian yang terkait dengan keterbukaan informasi bidang pertahanan dan dampak yang dihadapi pada era peperangan informasi dengan menimbang secara seimbang akibat negatif maupun positif untuk negara yang akan dijelaskan secara singkat sebagai berikut:

D. T. Kuehl. 2009. From Cyberspace to Cyberpower: Defining the Problem

Tulisan Kuehl adalah salah satu tulisan yang terdapat dalam buku terbitan National Defense University tahun 2009 yang bertema besar *Cyberpower and National Security.* F. D. Kramer, S. Starr, dan L. K. Wentz berlaku sebagai editor dalam kumpulan tulisan yang diterbitkan di Washington D. C., Amerika Serikat tersebut. Preposisi yang ditawarkan Kuehl dalam tulisannya adalah bahwa jaringan dan interkoneksi yang terhubung secara simultan tidak hanya dapat menjadi sarana dalam memenangkan peperangan asimetris saat ini, tetapi dalam sudut pandang yang lebih mendalam, Kuehl berargumen bahwa informasi yang tersebar di dunia siber dapat menimbulkan dampak di ruang fisik maupun ruang siber serta di luar maupun di dalam garis batas geografis. Dalam tulisannya Kuehl menekankan bahwa, ruang siber dapat menjadi sebuah wilayah peperangan karena ruang siber telah memiliki implikasi terhadap tiga dimensi yaitu dimensi fisik, dimensi informasi dan dimensi kognitif.

R. A. Clarke dan R. K. Knake. 2010. Cyber War: The Next Threat to National Security and What to Do About It

Tulisan Clarke dan Knake menjelaskan mengenai ruang siber yang dianggapnya sebagai sebuah ancaman bagi keamanan nasional sebuah negara. Clarke dan Knake memberikan beberapa contoh negara yang pernah menghadapi peperangan siber yang menjadi ancaman bagi keamanan

nasional negara. Tulisan tersebut juga membahas secara sistematis mengenai peristiwa yang mengakibatkan peperangan siber tersebut dan bagaimana negara tersebut menghadapi serangan siber. Di samping juga Clarke dan Knake menuliskan tentang kekurangan dari strategi yang diambil oleh negara-negara tersebut dan strategi apa yang dapat diambil sehingga kejadian serupa dapat diambil pelajarannya oleh negara lain.Selain itu, Clarke dan Knake lebih secara jelas menyatakan bahwa ruang siber memang merupakan wilayah peperangan kelima dalam kajian pertahanan dan keamanan. Beberapa argumen menarik yang dipaparkannya adalah; (1) perang siber adalah suatu peristiwa yang nyata dengan catatan bahwa apa yang saat ini terjadi pada negara seperti Estonia, Taiwan, dan Suriah tergolong masih sangat primitif dalam skala siber sehingga ancaman peperangan siber berikutnya akan lebih besar lagi, (2) Peperangan siber terjadi dengan kecepatan yang sangat tinggi dengan dibantu kabel *fiber-optic* sehingga jangka waktu antara dilancarkannya serangan tersebut dan dampak yang dihadapi sangat kecil. Hal inilah kerentanan yang harus diwaspadai oleh pembuat kebijakan, (3) Peperangan siber adalah sebuah perang global dengan keberadaan *server* yang tersebar di seluruh dunia dan mudahnya melakukan *defacing* dalam kasus *hacker,* (4) Peperangan siber dapat secara mudah melewati pertahanan tradisional negara dengan mudahnya melumpuhkan radar pertahanan udara atau melumpuhkan sistem di bank, (5) peperangan siber telah dimulai dan negara telah menjadi salah satu aktor aktif di dalamnya yang melakukan aksi *hacking* terhadap infrastruktur dan jaringan yang dimiliki negara lain. Jika aksi tersebut terjadi secara terus menerus maka akan menimbulkan pengaburan dalam definisi damai dan perang yang menciptakan dimensi baru ketidakstabilan.

Universitas Pertahanan Indonesia. 2012. Kajian Strategis Keamanan Cyber Nasional.

Tulisan yang diterbitkan oleh Tim Universitas Pertahanan Indonesia tersebut merupakan sebuah kajian akademis mengenai bidang peperangan informasi dan peperangan siber. Tulisan tersebut dipublikasikan pada seminar yang melibatkan Kementerian Pertahanan dan Kementerian Komunikasi dan Informatika dengan tema serupa dengan judul tulisan tersebut. Tulisan tersebut berpendapat bahwa dalam proses perumusan kebijakan pertahanan negara, terutama yang berkaitan dengan isu siber, perlu untuk dimasukkan sebagai bagian dari strategi pertahanan negara baik dalam rangka mencegah, menangkal ataupun mengatasinya. Dalam penyusunan konsep strategi tersebut perlu melibatkan sejumlah pemegang kebijakan terkait yang perlu ditindaklanjuti secara terkoordinasi. Selain perlu pula kebijakan tersebut disesuaikan dengan berbagai perundangan yang telah berlaku.

E. Schmidt dan J. Cohen. 2013. The New Digital Age.

Produksi tulisan karya Eric Schmidt dan Jared Cohen ini diterbitkan sebagai sebuah buku yang mendapat predikat ‘penjualan terbaik’ dari *New York Times* dan diterbitkan pada 2013. Tulisan tersebut secara provokatif dan menyeluruh menuliskan tentang pertanyaan terbesar mengenai masa depan umat manusia dengan keberadaan teknologi yang telah dapat mengubah cara manusia menghadapi persoalan mengenai privasi, keamanan, perang, intervensi, diplomasi, revolusi dan terorisme. Schmidt dan Cohen sebagai orang yang telah tumbuh bersama dengan Google menuangkan tulisannya tentang bagaimana informasi dan teknologi dapat menghancurkan kepentingan nasional suatu negara dan bagaimana agar dapat melakukan rekonstruksi jika hal tersebut benar terjadi. Kesimpulan yang disajikan Schmidt dan Cohen sangat menarik dengan mengangkat bagaimana harapan penjagaan rahasia dan privasi agar tiap individu, institusi dan negara

dapat berjalan secara baik. Dalam tesis ini, tulisan Schmidt dan Cohen menjadi referensi penting yang menyoroti bagaimana ancaman siber telah berevolusi dari waktu ke waktu dan menjadi semakin nyata bagi individu-individu maupun negara di dunia. Selain itu, tulisan ini menjadi referensi tambahan yang menyajikan tulisan mengenai siber melalui pendekatan lain di samping pendekatan teknis.

P.W Singer dan A. Friedman. 2014. Cybersecurity and Cyberwar: What Everyone Needs to Know.

Dalam buku yang ditulis oleh Singer dan Friedman, kajian mengenai peperangan informasi dan keamanan siber diangkat menjadi diskursus yang mudah dengan mengangkat contoh yang terjadi pada kehidupan sehari-hari, baik pada level individu, level institusi hingga level negara. Pertanyaan yang diajukan oleh buku ini sangat menyentuh terhadap pengetahuan masyarakat awam yakni; bagaimana peperangan informasi terjadi, mengapa hal tersebut sangat penting dan apa yang dapat kita lakukan untuk menghadapi hal tersebut. Tulisan ini disajikan dengan menarik dan menggabungkan sudut pandang keilmuan teknologi informasi dengan keilmuan hubungan internasional.

BAB 3

METODOLOGI PENELITIAN

3.1. Sumber Data/Subyek/Obyek Penelitian

3.1.1. Sumber Data Penelitian

Metodologi penelitian dalam tesis ini menggunakan metode kualitatif dengan sumber data utama (primer) adalah wawancara dan sumber data tambahan (sekunder) meliputi dokumen tertulis, foto, maupun data statistik[31]. Penelitian ini dilakukan dengan pendekatan legal formal yang dihubungkan dengan UU no. 14 tahun 2008 tentang keterbukaan informasi publik yang kemudian menggunakan analisis interpretasi-naratif[32] berdasarkan wawancara mendalam dan data sekunder. Data primer yang digunakan untuk mendukung penelitian ini diperoleh dari wawacara dengan Kementerian Komunikasi dan Informatika, Kementerian Pertahanan, Kementerian Riset dan Teknologi, pengamat militer, pengamat demokrasi, pengamat siber, dan akademisi. Selain itu wawancara juga akan dilakukan secara acak kepada masyarakat untuk memperoleh informasi terkait dengan keterbukaan informasi di Indonesia. Adapun data sekunder diperoleh dari buku, jurnal, artikel, maupun publikasi lainnya yang memiliki keterkaitan dengan penelitian ini. UU dan regulasi lainnya, serta sumber-sumber lainnya juga akan digunakan sebagai sumber pendukung data sekunder.

---

[31] L. J. Moleong, *Metode Penelitian Kualitatif*, PT. Remaja Rosdakarya, Bandung, 2010, hal 157.

[32] Dalam penelitian interpretatif, menurut Dvora Yanow dan Peregrine Schwartz-Shea dalam bukunya *Interpretive Research Design: Concepts and Proccesses*, digunakan untuk menganalisis mengenai kebijakan dan implementasi kebijakan tersebut. Menurt Yanow dan Schwart-Shea melalui metode ini peneliti dapat melakukan penafsiran dengan bebas. Hal ini dikarenakan penelitian ini benar-benar tergantung pada kemampuan dan pengetahuan yang dimilikinya dan tidak bersifat apriori. Selain itu, penelitian interpretatif cenderung lebih bersifat analitis.

3.1.2. Subyek Penelitian

Subyek dari penelitian ini adalah Kementerian Pertahanan, dan Kementerian Komunikasi dan Informatika.

3.1.3. Obyek Penelitian

Obyek penelitian mengenai pola keterbukaan informasi bidang pertahanan di Indonesia yang sesuai dengan UU no. 14 tahun 2008 dengan analisis sistem informasi pertahanan negara tersebut pada era peperangan informasi saat ini dan dikaitkan dengan konsep ancaman nontradisional.

3.2. Desain Penelitian

Desain penelitian ini didasarkan pada pesatnya kemajuan teknologi pada level global yang berpengaruh pada level nasional yang memungkinkan terjadinya peperangan yang melibatkan informasi pertahanan Indonesia. Dalam menanggapi hal tersebut, Indonesia belum memiliki pola dan implementasi sistem yang tepat untuk diterapkan dalam pengelolaan informasi bidang pertahanan. Sebagaimana UU mengatur mengenai keterbukaan informasi yang harus dilakukan setiap institusi yang anggarannya dibiayai oleh publik. Saat ini Indonesia memang telah memiliki pengaturan mengenai informasi pertahanan yang patut diketahui publik dan informasi apa yang tidak dapat diketahui publik. Namun, Indonesia belum memiliki pemetaan ancaman yang jelas terhadap sistem yang berlaku saat ini. Hal itu menimbang terutama pada faktor sangat dinamisnya sistem informasi saat ini. Oleh karena itu, peneliti perlu mengumpulkan data yang mendasari dari penelitian berupa data wawancara langsung yang dilakukan peneliti dengan beberapa unit kerja di Kementerian Komunikasi dan Informatika serta unit-unit kerja di Kementerian Pertahanan, data sekunder berupa presentasi, publikasi, dan dokumentasi yang diterbitkan oleh Kementerian Komunikasi dan Informatika serta Kementerian Pertahanan

mengumpulkan literatur, teori-teori sebagai landasan dalam penelitian. Sistem informasi yang jelas dengan pola kelola yang lebih tepat terhadap informasi bidang pertahanan dengan pertimbangan pada aspek ancaman tentu akan lebih menguntungkan Indonesia dalam menghadapi era peperangan informasi seperti saat ini.

3.3. Teknik Pengumpulan Data

Penelitian ini didasarkan pada penelitian kualitatif yang pencarian dan pengumpulan referensi ditekankan kepada pengambilan data berupa wawancara dengan narasumber, dan publikasi serta dokumentasi yang dimiliki oleh institusi-institusi terkait, pengumpulan literatur, dan kepustakaan. Data yang diproses digunakan untuk menemukan struktur, sistem, tindakan, dan perilaku yang tepat dalam keterbukaan informasi bidang pertahanan guna menghadapi ancaman nontradisional. Untuk lebih fokus dan terarah dalam penelitian, maka teknik pengumpulan data adalah sebagai berikut:

3.3.1. Studi pustaka (Library Research)

Studi pustaka dilakukan dengan cara menelaah dan membandingkan beberapa buku untuk memperoleh data yang bersifat teoritis sebagai data primer yang terdiri dari teori-teori tentang keamanan, strategi dalam peperangan informasi, dan bahan kepustakaan lainnya terkait dengan permasalahan yang diangkat dalam penelitian ini. Selain itu peneliti akan mencari data-data pendukung seperti dokumen, arsip, surat keputusan, dan berkas lain dari institusi terkait seperti Kementerian Pertahanan, Kementerian Komunikasi dan Informatika, Dinas Informasi dan Pengolahan Data TNI, LIPI, dan sebagainya.

3.3.2. Wawancara Mendalam (In-Depth Interview)

Dengan metode wawancara diharapkan akan diperoleh informasi yang mendalam, optimal, dan obyektif terkait dengan strategi Indonesia dalam

melindungi informasi vital bidang pertahanan dalam era peperangan informasi. Dengan menggunakan wawancara, diharapkan peneliti akan mendapat informasi dan data yang diinginkan serta bahan-bahan dan gambaran yang lebih obyektif tentang masalah yang diselidiki. Adapun yang menjadi narasumber adalah mereka yang terlibat langsung dalam sistem informasi bidang pertahanan, para pengamat, serta akademisi. Namun selain melakukan wawancara mendalam, peneliti juga melakukan *limited discussion* dengan terdapat beberapa narasumber di dalamnya.

3.4. Teknik Penentuan Informan (Narasumber).

Peneliti akan melaksanakan wawancara mendalam (*In-Depth Interview)* dengan para informan yaitu orang-orang yang berperan penting, yang memiliki pengetahuan yang luas tentang daerah penelitian, dan yang berkenan untuk bekerjasama dalam kegiatan penelitian dengan cara *purposive* melalui penentuan informan yang telah dilakukan sebelumnya. Informan yang dimaksud antara lain aparat pemerintah yang berperan dalam pembuatan sistem informasi bidang pertahanan dan penerapan kebijakan yang mengenainya, seperti Sekretaris Jenderal Kementerian Pertahanan, Kepala Pusat Komunikasi Publik Kementerian Pertahanan, Kepala Pusat Data dan Informasi Kementerian Pertahanan, Direktur Keamanan Informasi Kementerian Komunikasi dan Informatika, Kepala Dinas Informasi dan Pengolahan Data TNI-AD, Anggota Komisi Informasi Pusat, dan akademisi.

3.5. Prosedur Pengolahan Data

Pengolahan atau analisis data kualitatif dilakukan dengan jalan bekerja dengan data, mengorganisasikan data, memilah-milahnya menjadi satuan yang dapat dikelola, mensintesiskannya, mencari dan menemukan pola, menemukan apa yang penting dan apa yang dipelajari, dan memutuskan apa yang dapat diceritakan kepada orang lain. Pengolahan data seperti yang disampaikan di atas, dilakukan dengan:

1. *Data Reduction Process* (reduksi data), yaitu data yang diperoleh direduksi, dirangkum, dan dipilih sesuai dengan tema yang akan diangkat sesuai dengan permasalahan yang diteliti. Selanjutnya data-data tersebut difokuskan terhadap hal-hal yang relevan dengan penelitian.
2. *Data Display Process* (penyajian data), yaitu susunan informasi yang memungkinkan dapat ditariknya suatu kesimpulan dapat berupa matriks untuk memudahkan untuk pemahaman permasalahan.
3. *Data Analysis,* dalam hal ini data yang diperoleh dihubungkan dengan teori dianalisis dengan data yang ada[33] sesuai dengan permasalahan yang diangkat sehingga dapat memahami permasalahan secara lebih komprehensif.
4. *Conclusion Verification Process* (penarikan kesimpulan), yaitu suatu kesimpulan yang diverifikasi dengan cara melihat dan mempertanyakan kembali, dengan meninjau kembali secara sepintas pada catatan lapangan untuk memperoleh pemahaman yang lebih cepat.
5. *Mengingkatkan keabsahan data,* proses ini data tersebut diteliti kembali seperti melakukan triangulasi yaitu mengecek keabsahan data dengan sumber lain dan melakukan diskusi.
6. *Narasi,* data yang diperoleh dinarasikan sehingga berupa uraian-uraian lebih lanjut mengenai data yang diperoleh.

[33] J. W. Creswell,*Research Design Pendekatan Kualitatif, Kuantitatif, dan Mixed.* Pustaka Pelajar, Yogyakarta, 2010, hal 275.

BAB 4

DATA DAN ANALISIS PENELITIAN

4.1. Hasil Penelitian

Hasil yang diperoleh dalam penelitian ini berkaitan dengan pola keterbukaan informasi pertahanan di Indonesia yang dilakukan oleh beberapa institusi yang terkoordinasi seperti Kementerian Komunikasi dan Informatika dan Kementerian Pertahanan yang di dalamnya meliputi Markas Besar TNI serta identifikasi ancaman non-tradisional terhadap informasi pertahanan tersebut.

4.1.1. Gambaran Umum Pola Keterbukaan Informasi di Indonesia

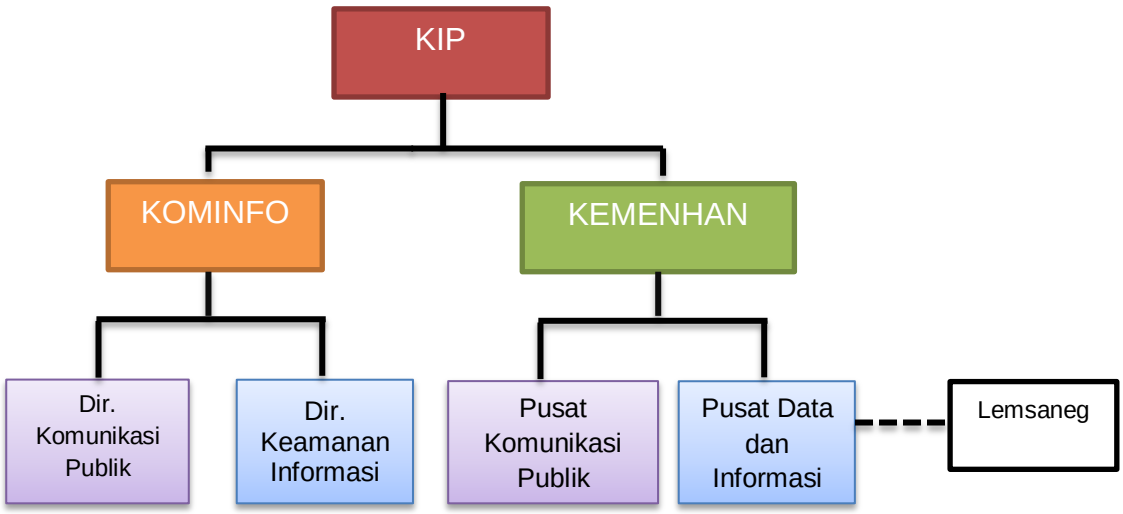
Di Indonesia, informasi menjadi suatu hal yang sangat penting dan pengaturannya telah ditulis dalam Undang-Undang Dasar 1945 (UUD 1945) pada pasal 28f yang berisikan sebagai berikut,

> "Setiap orang berhak untuk berkomunikasi dan memperoleh informasi untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, menyampaikan informasi dengan mnggunakan segala jenis saluran yang tersedia".

Amanat UUD 1945 tersebutlah yang memberikan amanat pada institusi-institusi pemerintah untuk merumuskan, menyusun, serta mengimplementasikan kebijakan mengenai informasi. Terutama mengenai informasi bidang pertahanan yang merupakan informasi kritis bagi setiap negara. Di Indonesia, informasi bidang pertahanan diatur oleh dua kementerian yang di bawahnya didiferensiasi sesuai dengan fungsi dan perannya.[34] Sesuai gambar 4.1., bahwa kementerian yang bertanggungjawab terhadap pola keterbukaan informasi pertahanan adalah Kementerian

[34] Wawancara dengan Sekretaris Jenderal Kementerian Pertahanan pada 24 November 2014 pukul 15.30 WIB di Kementerian Pertahanan, Jakarta Pusat.

Komunikasi dan Informatika sebagai kementerian yang secara umum mengatur tata kelola berbagai informasi publik beserta dengan Kementerian Pertahanan yang secara khusus mengatur tata kelola informasi pertahanan.



Gambar 4.1 Pola Keterbukaan Informasi Pertahanan

Dalam menentukan regulasi dan sistem keamanan tiap informasi yang dimiliki oleh institusi di Indonesia, Kementerian Komunikasi dan Informatika menjadi kementerian yang berperan sangat penting untuk menjamin tersedianya informasi publik yang dibutuhkan oleh masyarakat sebagai bentuk pengawasan terhadap pemerintahan yang baik. Di sisi lain, Kementerian Komunikasi dan Informatika juga bertanggungjawab untuk menjamin bahwa informasi publik yang tidak seharusnya diketahui publik aman dari pihak yang tidak memiliki otorisasi untuk mengetahuinya. Secara spesifik, informasi bidang pertahanan memiliki karakteristik pola keterbukaan informasi yang berbeda dibandingkan dengan pola keterbukaan yang dimiliki oleh kementerian lain. Dalam menangani keamanan informasi pertahanan tersebutlah, Kementerian Komunikasi dan Informatika melakukan koordinasi dengan Kementerian Pertahanan sebagai pelaksana fungsi pemerintah di bidang pertahanan, baik pertahanan militer maupun nirmiliter.

Telah disebutkan sebelumnya bahwa Indonesia menjamin hak warga negaranya untuk mendapatkan informasi melalui sebuah pasal di Undang-Undang Dasar. Berdasarkan UU tersebut, diturunkanlah Peraturan Pemerintah no. 61 tahun 2010 tentang pelaksanaan UU no. 14 tahun 2008 tentang keterbukaan informasi publik. Peraturan Pemerintah tersebut ditetapkan pada 20 Agustus 2010 dan berlaku untuk setiap lembaga eksekutif, legislatif, yudikatif, dan badan lain yang fungsi dan tugas pokoknya berkaitan dengan penyelenggaraan negara, yang sebagian atau seluruh dananya bersumber dari Anggaran Pendapatan dan Belanja Negara dan/atau Anggaran Pendapatan dan Belanja daerah, atau organisasi nonpemerintah sepanjang sebagian atau seluruh dananya bersumber dari Anggaran Pendapatan dan Belanja Negara dan/atau Anggaran Pendapatan dan Belanja Daerah, sumbangan masyarakat, atau dari luar negeri. Dengan UU tersebut, secara resmi Indonesia menjadi negara kelima di Asia yang menjamin warga negara untuk mendapatkan informasi publik.[35]

Di dalamnya mengatur pula hak keterbukaan informasi tersebut yang meliputi: (1). Hak publik untuk memantau atau mengamati perilaku pejabat publik dalam menjalankan fungsi publiknya (*right to observe*); (2). Hak publik untuk mendapatkan/mengakses informasi *(public access to information*); (3). Hak publik untuk berpartisipasi dalam proses pembentukan kebijakan (*right to participate*); (4). Kebebasan berekspresi yang salah satunya diwujudkan kebebasan pers (*free and responsible pers*); (5). Hak publik untuk mengajukan keberatan apabila hak-hak di atas diabaikan (*right to appeal*) baik melalui administrasi maupun *adjudikasi* (menggunakan sarana pengadilan semu, arbitrasi maupun pengadilan). Melalui UU yang sama pula diatur bahwa hak tersebut dijamin dengan dibentuknya sebuah unit kerja tersendiri yang berfungsi untuk menjalankan UU tersebut dan mengatur pelaksanaannya, menetapkan petunjuk teknis standar pelayanan informasi

[35] M. Ali Sera, 'Membangun Kesadaran Informasi Publik', dalam Afriadi dan B. Hersutanto (eds.), *Indonesia Berdaulat Bermartabat: Kompilasi Pemikiran Anggota Komisi I DPR RI 2009-2014*, RMBooks, Jakarta, 2014, hal.302.

publik dan menyelesaikan sengketa informasi publik melalui mediasi atau ajudikasi nonlitigasi.[36]

Komisi Informasi Pusat dan memiliki tanggung jawab langsung pada presiden. Informasi yang dijamin oleh Komisi Informasi Publik dan wajib untuk disediakan dan diumumkan diklasifikasikan menjadi tiga jenis; (1) Informasi yang wajib disediakan dan diumumkan secara berkala yaitu informasi yang harus dikeluarkan secara berkala paling cepat selama enam bulan sekali seperti informasi yang berkaitan dengan badan publik, informasi mengenai kegiatan dan kinerja badan publik terkait, informasi mengenai laporan keuangan dan/atau informasi lain yang diatur dalam peraturan perundang-undangan; (2) Informasi yang wajib diumumkan secara serta-merta yaitu informasi yang dianggap dapat mengancam hidup orang banyak dan ketertiban umum, dapat diketahui oleh semua warga negara seperti informasi tentang bencana alam, bencana non-alam, bencana konflik sosial, serta penyakit epidemik; (3) Informasi yang wajib tersedia setiap saat seperti seluruh informasi publik yang berada di bawah penguasaan badan publik, tidak termasuk informasi yang dikecualikan, seperti rencana kerja proyek termasuk di dalamnya perkiraan pengeluaran tahunan badan publik, dan informasi tentang kebijakan yang disampaikan pejabat publik dalam pertemuan yang terbuka untuk umum.

Jika regulasi tersebut adalah regulasi yang berlaku secara nasional bagi setiap badan publik yang ada di Indonesia, maka informasi pertahanan yang dikelola oleh Kementerian Pertahanan memiliki pola regulasi yang lebih spesifik. Dengan adanya UU no. 14 tahun 2008 tentang keterbukaan publik, Kementerian Pertahanan melalui Pusat Komunikasi Publik menjadi pihak yang bertanggungjawab untuk menjamin keterbukaan informasi publik bagi masyarakat. Informasi-informasi yang wajib disediakan oleh Kementerian Pertahanan sebagai bagian dari informasi bidang pertahanan ditulis dalam

[36] Kementerian Komunikasi dan Informatika Republik Indonesia, *Undang-Undang Republik Indonesia No.14 Tahun 2008 tentang Keterbukaan Informasi Publik*, Kementerian Komunikasi dan Informatika Republik Indonesia, 2013, hal. 3.

Lampiran Keputusan Menteri Pertahanan KEP/538/M/VII/2012.[37] Sedangkan untuk menjamin tersedianya adanya data yang dibutuhkan secara internal ke dalam Kementerian Pertahanan, Pusat Data dan Informasi menyediakan sebuah sistem yang berbasis desain yang digunakan untuk membangun dan memperkaya suatu sistem berbasis teknologi informasi yang dapat memberikan layanan data dan informasi dalam rangka mendukung penyelenggaraan pertahanan negara yang meliputi layanan internal untuk tercapainya tujuan reformasi birokrasi menuju ke pemerintahan yang baik dan layanan publik di lingkungan Kementerian Pertahanan dan TNI. Sistem tersebut dinamakan Sistem Informasi Pertahanan Negara (Sisfohanneg). Sisfohanneg sendiri merupakan sistem yang sedang dibangun dan dikembangkan Kementerian Pertahanan dengan sifat sistem yang satu kesatuan dan diharapkan dapat terintegrasi sebagai sistem informasi nasional.[38]

Meskipun UU no. 14 tahun 2008 telah menuliskan mengenai informasi apa saja yang diperbolehkan untuk diungkap kepada publik, tetapi untuk melindungi kerahasiaan, keutuhan, dan ketersediaan aset informasi Kementerian Pertahanan dan TNI dari berbagai bentuk ancaman keamanan informasi, baik dari dalam maupun luar lingkungan, perlu melakukan pengecualian terhadap beberapa informasi bidang pertahanan. UU no. 14 tahun 2008 tersebut juga menuliskan hak badan publik termasuk Kementerian Pertahanan untuk menolak memberikan informasi jika informasi yang diminta adalah informasi yang dikecualikan dan jika informasi publik yang diminta tidak sesuai dengan perundang-undangan. Informasi bidang pertahanan yang dikecualikan adalah; (1) Informasi yang dapat menghambat proses penegakan hukum; (2) Informasi yang berkaitan dengan kepentingan

[37] Lihat Lampiran 4.

[38] Wawancara dengan Kepala Bidang Informasi dan Persandian merangkap Kepala Bidang Pengembangan Sistem Informasi Pertahanan pada 1 Desember 2014 pukul 09.30 WIB di Kantor Pusat Data dan Informasi Kementerian Pertahanan, Jakarta Selatan.

perlindungan hak atas kekayaan intelektual dan perlindungan dari persaingan usaha tidak sehat; (3) Informasi yang membahayakan pertahanan negara; (4) Informasi yang merugikan ketahanan ekonomi nasional; (5) Informasi tentang akta otentik yang bersifat pribadi; (6) Informasi yang berkaitan dengan rahasia jabatan; (7) Memorandum atau surat-surat antar Badan Publik atau intra Badan Publik yang menurut sifatnya dirahasiakan, kecuali atas putusan Komisi Informasi atau pengadilan. Informasi Publik yang diminta belum dikuasai atau didokumentasikan. Informasi yang dikecualikan tersebut bersifat rahasia dan diatur dengan UU didasarkan pada pengujian tentang konsekuensi yang timbul apabila suatu informasi diberikan kepada masyarakat serta setelah dipertimbangkan dengan seksama bahwa menutup informasi tersebut dapat melindungi kepentingan yang lebih besar daripada membukanya atau sebaliknya.

Jenis-jenis informasi bidang pertahanan yang dilarang untuk diketahui publik dan tergolong sebagai informasi yang dikecualikan, diantaranya;

(1) Informasi tentang strategi, intelijen, operasi, taktik dan teknik yang berkaitan dengan penyelenggaraan sistem pertahanan dan keamanan negara, meliputi tahap perencanaan, pelaksanaan dan pengakhiran atau evaluasi dalam kaitan dengan ancaman dari dalam dan luar negeri;

(2) Dokumen yang memuat tentang strategi, intelijen, operasi, teknik dan taktik yang berkaitan dengan penyelenggaraan sistem pertahanan dan keamanan negara yang meliputi tahap perencanaan, pelaksanaan dan pengakhiran atau evaluasi;

(3) Jumlah, komposisi, disposisi, atau dislokasi kekuatan dan kemampuan dalam penyelenggaraan sistem pertahanan dan keamanan negara serta rencana pengembangannya;

(4) Gambar dan data tentang situasi dan keadaan pangkalan dan/atau instalasi militer;

(5) Data perkiraan kemampuan militer dan pertahanan negara lain terbatas pada segala tindakan dan/atau indikasi negara tersebut yang dapat

membahayakan kedaulatan Negara Kesatuan Republik Indonesia dan/atau data terkait kerjasama militer dengan negara lain yang disepakati dalam perjanjian tersebut sebagai rahasia atau sangat rahasia;

(6) Sistem persandian negara; dan/atau

(7) Sistem intelijen negara. Berdasarkan UU no. 14 tahun 2008 tersebut pula Kementerian Pertahanan mengeluarkan surat keputusan KEP/1040/M/XII/2011 pada 30 Desember 2011 mengenai detil informasi pertahanan apa saja yang dianggap sebagai informasi yang dikecualikan.[39]

Selain mengatur informasi yang patut untuk diketahui publik dan informasi yang dikecualikan untuk diketahui oleh publik, UU no. 14 tahun 2008 juga mengatur mengenai hukuman yang dapat dikenakan kepada pihak-pihak yang berusaha untuk mengakses, menggunakan, atau mengumumkan mengenai informasi yang dikecualikan tersebut. Beberapa ketentuan pidana yang dicantumkan dalam regulasi keterbukaan informasi pertahanan diantaranya adalah bagi pihak-pihak yang melakukan tindakan berikut; (1) Badan Publik yang dengan sengaja tidak menyediakan, tidak memberikan, dan/atau tidak menerbitkan Informasi Publik berupa Informasi Publik secara berkala, Informasi Publik yang wajib diumumkan secara serta-merta, Informasi Publik yang wajib tersedia setiap saat, dan/atau Informasi Publik yang harus diberikan atas dasar permintaan sesuai dengan Undang-Undang ini, dan mengakibatkan kerugian bagi orang lain; (2) Dengan sengaja dan melawan hukum menghancurkan, merusak, dan/atau menghilangkan dokumen Informasi Publik dalam bentuk media apa pun yang dilindungi Negara dan/atau yang berkaitan dengan kepentingan umum; (3) Dengan sengaja dan tanpa hak mengakses dan/atau memperoleh dan/atau memberikan informasi yang dikecualikan; (4) Dengan sengaja dan tanpa hak mengakses dan/atau memperoleh dan/atau memberikan informasi yang dikecualikan; (5) Dengan sengaja membuat Informasi Publik yang tidak benar atau menyesatkan dan mengakibatkan kerugian bagi orang lain.

[39] Lihat Lampiran 5.

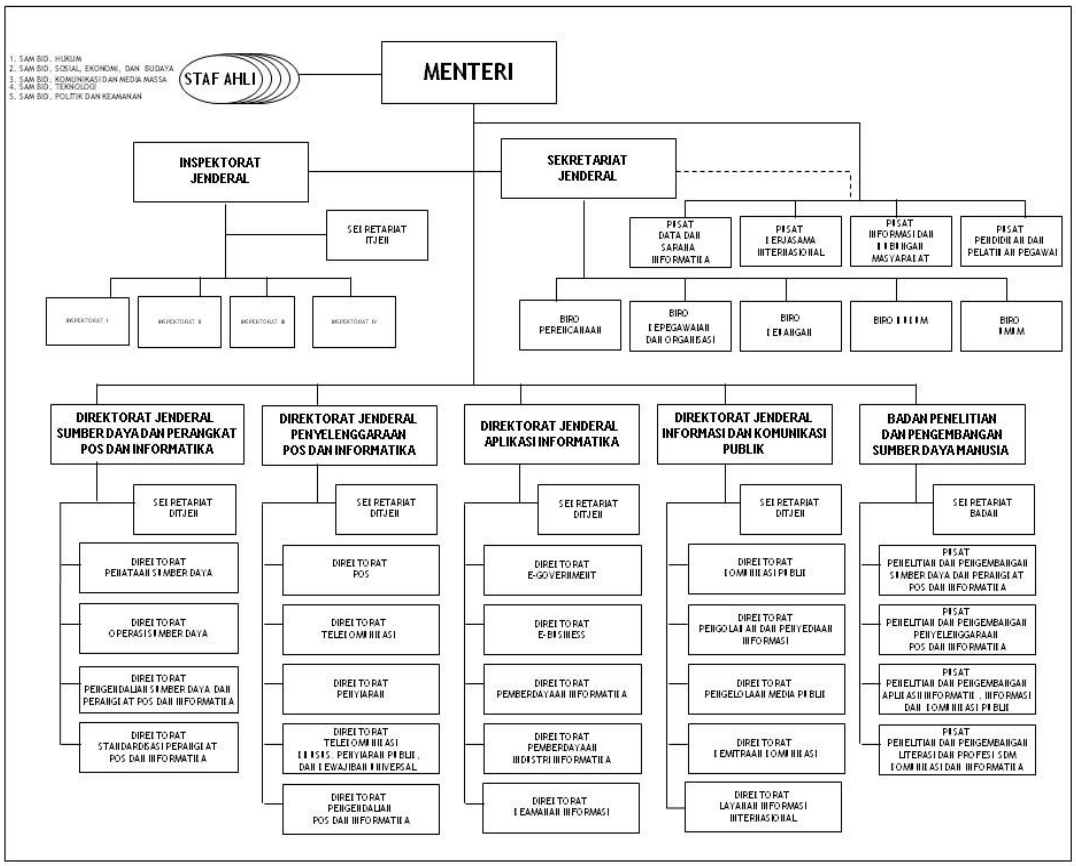
4.1.2 Peran Kementerian Komunikasi dan Informatika

Kementerian Komunikasi dan Informatika secara umum merupakan kementerian yang mempunyai tugas untuk menyelenggarakan urusan di bidang komunikasi dan informatika dalam pemerintahan Indonesia sebagai upaya membantu Presiden dalam menyelenggarakan pemerintahan negara. Dalam Peraturan Menteri Komunikasi dan Informatika nomor: 17/per/m.kominfo/10/2010 tentang organisasi dan tata kerja Kementerian Komunikasi dan Informatika dinyatakan bahwa Kementerian Komunikasi dan Informatika memiliki fungsi berikut;

(1) Perumusan, penetapan, dan pelaksanaan kebijakan di bidang komunikasi dan informatika;
(2) Pengelolaan barang milik atau kekayaan negara yang menjadi tanggung jawab Kementerian Komunikasi dan Informatika;
(3) Pengawasan atas pelaksanaan tugas di lingkungan Kementerian Komunikasi dan Informatika;
(4) Pelaksanaan bimbingan teknis dan supervisi atas pelaksanaan urusan Kementerian Komunikasi dan Informatika di daerah; dan
(5) Pelaksanaan kegiatan teknis yang berskala nasional.

Dari tugas dan fungsi tersebut, dapat dilihat pada gambar 4.2., Kementerian Komunikasi dan Informatika terbagi menjadi tujuh unit kerja yaitu; (1) Sekretariat Jenderal; (2) Direktorat Jenderal Sumber Daya dan Perangkat Pos dan Informatika; (3) Direktorat Jenderal Penyelenggaraan Pos dan Informatika; (4) Direktorat Jenderal Aplikasi Informatika; (5) Direktorat Jendral Informasi dan Komunikasi Publik; (6) Badan Penelitian dan Pengembangan Sumber Daya Manusia; dan (7) Inspektorat Jenderal. Melalui ketujuh unit kerja tersebut, dua direktorat berhubungan langsung dengan pengaturan dan implementasi terhadap pola keterbukaan informasi pertahanan di Indonesia. Kedua unit kerja tersebut adalah Direktorat Jenderal Aplikasi Informatika dan Direktorat Jendral Informasi dan Komunikasi Publik.

Direktorat yang berada di bawah Direktorat Jenderal Aplikasi Informatika dengan tugas untuk menjamin aspek-aspek keamanan informasi pertahanan di Indonesia adalah Direktorat Keamanan Informasi. Sedangkan Direktorat Komunikasi Publik yang berada di bawah Direktorat Jendral Informasi dan Komunikasi Publik memiliki tugas utama untuk menjamin bahwa hak masyarakat Indonesia untuk mengakses informasi pertahanan yang diperbolehkan sesuai dengan yang diatur oleh Peraturan Pemerintah no. 61 tahun 2010 tentang pelaksanaan UU no. 14 tahun 2008 tentang keterbukaan informasi publik.



Gambar 4.2. Struktur Organisasi
Kementerian Komunikasi dan Informatika[40]

[40] Sumber: Pejabat Pengelola Informasi dan Dokumentasi, *Struktur Organisasi (online),* <http://ppid.kominfo.go.id/about/kemkominfo/struktur/>, diakses pada 27 Desember 2014.

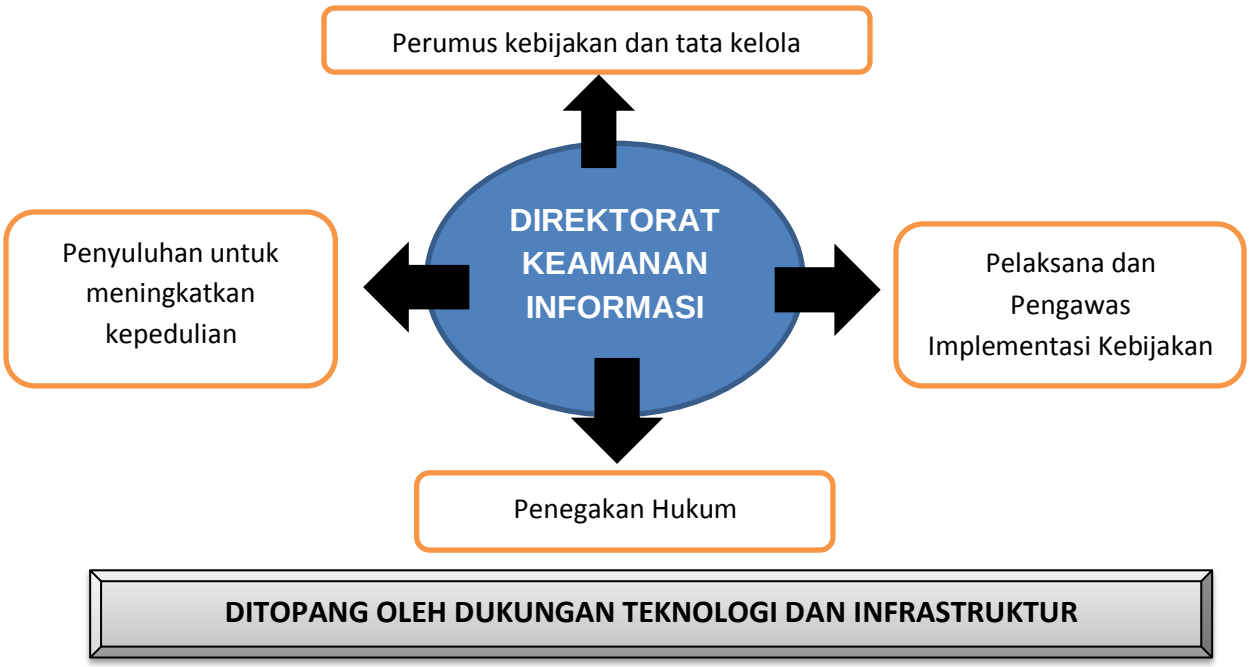
4.1.2.1. Direktorat Keamanan Informasi

Menurut Peraturan Menteri Komunikasi dan Informatika nomor: 17/per/m.kominfo/10/2010 pada pasal 465 hingga pasal 466 dinyatakan bahwa Direktorat Keamanan Informasi mempunyai tugas melaksanakan perumusan dan pelaksanaan kebijakan, penyusunan norma, standar, prosedur, dan kriteria, serta pemberian bimbingan teknis dan evaluasi di bidang keamanan informasi. Sedangkan menurut Peraturan Menteri tersebut juga diatur bahwa dalam melaksanakan tugasnya, direktorat tersebut memiliki fungsi berikut; (1) Perumusan kebijakan di bidang strategi dan kerjasama keamanan informasi, teknologi keamanan informasi, penanganan insiden, penyidikan dan penindakan, dan budaya keamanan informasi; (2) Pelaksanaan kebijakan di bidang strategi dan kerjasama keamanan informasi, teknologi keamanan informasi, penanganan insiden, penyidikan dan penindakan, dan budaya keamanan informasi; (3) Perumusan norma, standar, prosedur, dan kriteria di bidang strategi dan kerjasama keamanan informasi, teknologi keamanan informasi, penanganan insiden, penyidikan dan penindakan, dan budaya keamanan informasi; (4) Pemberian bimbingan teknis di bidang strategi dan kerjasama keamanan informasi, teknologi keamanan informasi, penanganan insiden, penyidikan dan penindakan, dan budaya keamanan informasi; (5) Pelaksanaan evaluasi penyelenggaraan kegiatan di bidang strategi dan kerjasama keamanan informasi, teknologi keamanan informasi, penanganan insiden, penyidikan dan penindakan, dan budaya keamanan informasi; dan (6) Pelaksanaan urusan tata usaha, kepegawaian, dan rumah tangga direktorat.

Untuk menjalankan tugasnya tersebut, terdapat masing-masing bidang tugas yang dikepalai oleh seorang kepala sub direktorat yang memiliki tugas yang spesifik.[41] Bidang-bidang tugas itu meliputi; (1) Tata Kelola Keamanan Informasi; (2) Teknologi Keamanan Informasi; (3) Monitoring, Evaluasi, dan

[41] Paparan Direktur Keamanan Informasi, Kementerian Komunikasi dan Informasi pada 6 Juli 2011 di Hotel Salak, Bogor.

Tanggap Darurat Keamanan Informasi; (4) Penyidikan dan Penindakan; (5) Budaya Keamanan Informasi. Pembagian bidang tugas itu disesuaikan dengan tujuan yang ingin dicapai oleh Direktorat Keamanan Informasi sebagai sebuah kesatuan institusi yaitu; (1) Menyusun kebijakan nasional di bidang keamanan informasi melalui kerjasama antar lembaga baik dalam maupun luar negeri; (2) Membangun kemampuan teknis di bidang teknologi keamanan informasi; (3) Menyelenggarakan penanganan insiden keamanan informasi nasional; (4) Menyelenggarakan penegakan hukum bidang Informasi dan Transaksi Elektronik; (5) Membangun budaya keamanan di dunia siber.



Gambar 4.3. Skema Kerja Direktorat Keamanan Informasi[42]

Berdasarkan gambar 4.3. tentang uraian tugas, fungsi dan skema kerja yang dimiliki oleh Direktorat Keamanan Informasi dapat diketahui bahwa direktorat tersebut memiliki struktur kompleks yang dibentuk untuk menjamin keamanan informasi, terutama informasi yang tidak boleh diketahui

[42] Sumber: Paparan Direktur Keamanan Informasi, Kementerian Komunikasi dan Informasi yang telah diolah oleh peneliti.

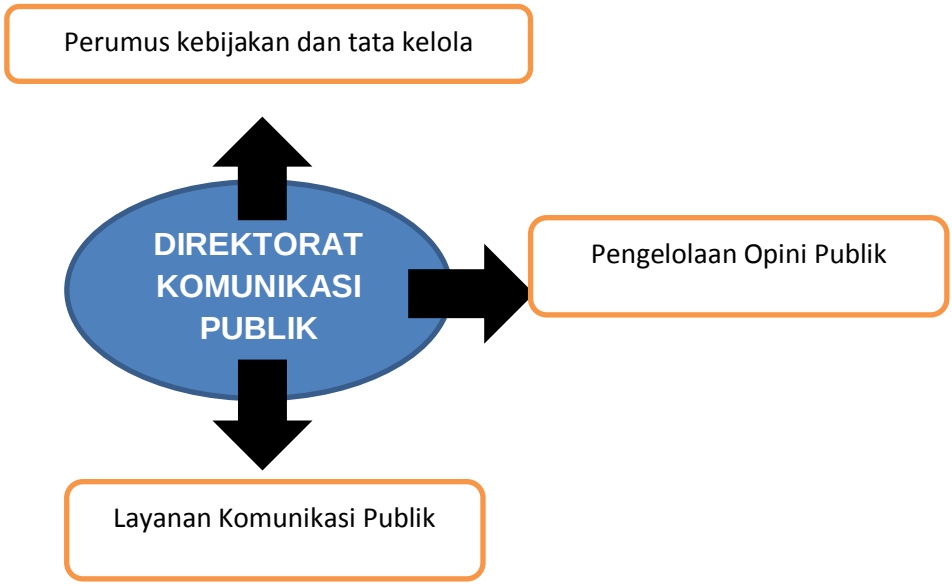
oleh publik seperti informasi pertahanan. Dalam tugas yang dijalankan oleh Direktorat Keamanan Informasi, terdapat tiga aspek yang sangat penting dalam hal menjamin keamanan informasi pertahanan yaitu[43]; (1) Terjaminnya kerahasiaan karena aspek ini berkaitan dengan pembatasan akses ke informasi yang hanya boleh diakses oleh pihak yang memiliki otorisasi untuk melakukannya; (2) Terjaminnya integritas karena aspek ini berkaitan dengan keakuratan dan kelengkapan sebuah informasi dan metode pemrosesannya; (3) Terjaminnya ketersediaan informasi jika pihak yang memiliki otorisasi berusaha untuk mengakses informasi tersebut. Peneliti menilai bahwa dalam melindungi keamanan informasi pertahanan yang dimiliki Indonesia, direktorat ini menjadi salah satu aktor penting di Kementerian Komunikasi dan Informatika yang dapat menjamin keamanan informasi melalui proses identifikasi, pengukuran, pengelolaan, dan pengontrolan terhadap resiko ancaman non-tradisional yang dapat muncul.

4.1.2.2. Direktorat Komunikasi Publik

Direktorat Komunikasi Publik menurut pasal 490 hingga 491 dari Peraturan Menteri Komunikasi dan Informatika nomor: 17/per/m.kominfo/10/2010 merupakan direktorat yang berada di bawah Direktorat Jenderal Komunikasi dan Informatika dan mempunyai tugas merumuskan serta melaksanakan kebijakan serta standardisasi teknis di bidang informasi, komunikasi publik, dan hubungan masyarakat pemerintah. Dalam menjalankan tugas-tugas tersebut, Direktorat Komunikasi Publik memiliki fungsi yang spesifik yaitu; (1) Penyiapan perumusan dan pelaksanaan kebijakan di bidang komunikasi publik; (2) Penyiapan penyusunan norma, standar, prosedur, dan kriteria di bidang komunikasi publik; (3) Penyiapan pemberian bimbingan teknis dan evaluasi di bidang komunikasi publik; dan (4) Pelaksanaan urusan tata usaha, kepegawaian,

[43] Kementerian Komunikasi dan Informatika, *Panduan Topologi dan Keamanan Sistem Informasi*, Kementerian Komunikasi dan Informatika, 2013, hal. 3.

dan rumah tangga direktorat. Pada tataran yang lebih kecil, Direktorat Komunikasi Publik terdiri atas beberapa sub bidang yaitu; (1) Tata Kelola Komunikasi Publik; (2) Pengelolaan Opini Publik; (3) Layanan Komunikasi Publik.



Gambar 4.4. Skema Kerja Direktorat Komunikasi Publik[44]

Berdasarkan uraian tugas, fungsi dan skema kerja pada gambar 4.4. yang dimiliki oleh Direktorat Keamanan Informasi dapat diketahui bahwa direktorat tersebut memiliki fokus untuk menjamin tersedianya perangkat regulasi yang tepat untuk tersedianya informasi publik, di samping juga mengelola opini yang ada di publik mengenai berbagai informasi yang berkaitan dengan pemerintahan maupun informasi yang dianggap berguna bagi berjalannya pemerintahan. Selain itu direktorat tersebut juga memberikan penyiapan, pemberian bimbingan teknis dan evaluasi terhadap layanan komunikasi publik yang dimiliki kementerian maupun lembaga non-kementerian. Direktorat ini menjadi salah satu aktor penting di Kementerian Komunikasi dan Informatika selain Direktorat Keamanan Informasi karena Direktorat Komunikasi Publik inilah yang memberikan jalur antara informasi

[44] Gambar telah diolah oleh peneliti.

pertahanan yang patut untuk diketahui oleh publik sehingga membantu menciptakan saling percaya dan meniadakan potensi konflik, namun di sisi lain memberikan pembatas untuk informasi pertahanan yang tidak patut diketahui oleh masyarakat luas. Di samping itu direktorat ini juga menjadi institusi yang dapat menjamin hak masyarakat dapat mengetahui informasi publik bidang pertahanan.

4.1.3. Peran Kementerian Pertahanan

Kementerian Pertahanan adalah sebuah kementerian yang secara umum mempunyai tugas menyelenggarakan urusan di bidang pertahanan dalam pemerintahan untuk membantu Presiden dalam menyelenggarakan pemerintahan negara. Menurut Peraturan Menteri Pertahanan Nomor:16 Tahun 2010[45] tentang Susunan Organisasi dan Tata Kerja Departemen Pertahanan Republik Indonesia tentang tugas dan fungsi Kementerian Pertahanan dicantumkan bahwa untuk menjalankan tugas tersebut, Kementerian Pertahanan menyelenggarakan fungsi;

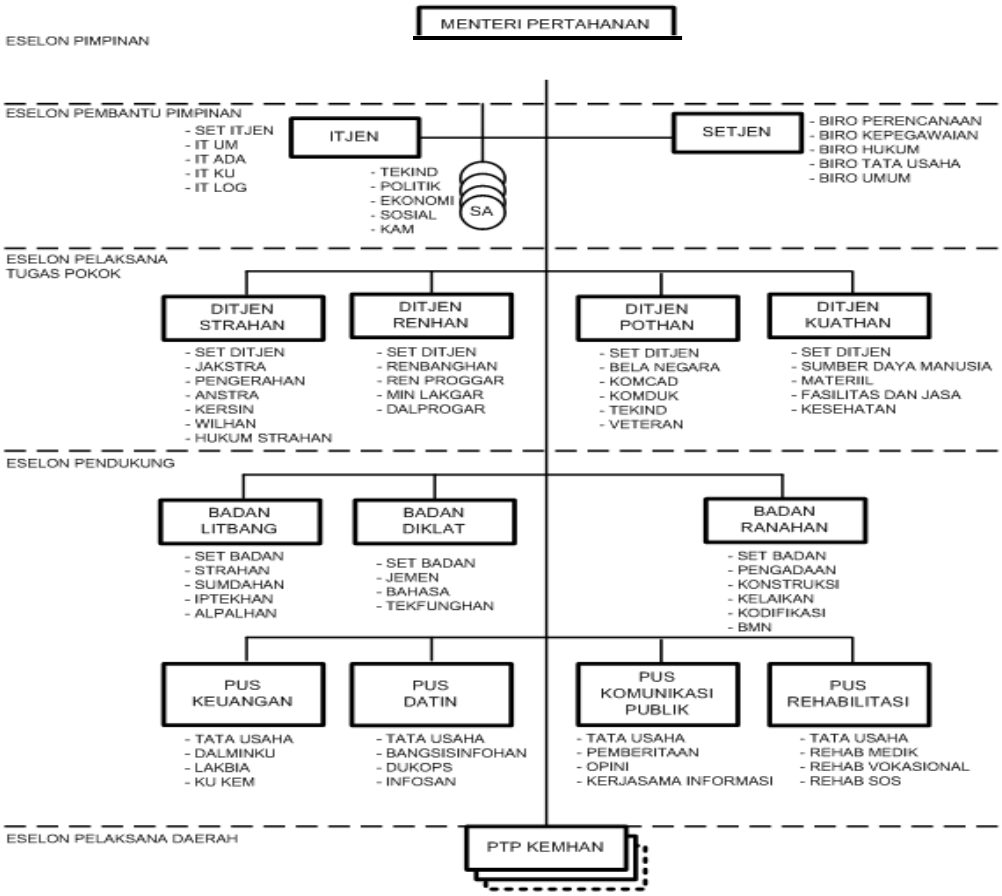
(1) Perumusan, penetapan, dan pelaksanaan kebijakan di bidang pertahanan;

(2) Pengelolaan barang milik atau kekayaan negara menjadi tanggungjawab Kementerian Pertahanan,

(3) Pengawasan atas pelaksanaan tugas di lingkungan Kementerian Pertahanan,

(4) Pelaksanaan kegiatan teknis dari pusat sampai ke daerah.

[45] Peraturan Menteri Pertahanan Nomor:16 Tahun 2010 adalah peraturan menteri yang mengganti Peraturan Menteri Per/01/M/VIII/2005 yang sebelumnya terbit. Hal tersebut dilaksanakan karena masih adanya fungsi yang belum terwadahi, memisahkan fungsi perumus kebijakan dan pelaksana kebijakan serta pengelompokan fungsi dalam peraturan menteri sebelumnya.



Gambar 4.5. Struktur Organisasi Kementerian Pertahanan[46]

Melalui gambar 4.5. tentang tugas yang dimiliki dan penyelenggaraan fungsi tersebut, Kementerian Pertahanan terdiri dari empat eselon[47] yaitu; (1) Eselon Pimpinan yang merupakan Menteri Pertahanan; (2) Eselon Pembantu Pimpinan yang terdiri dari Sekretariat Jenderal, Staf Ahli Menteri dan Inspektorat Jenderal; (3) Eselon Pelaksana Tugas Pokok yang terdiri dari Direktorat Jenderal Strategi Pertahanan, Direktorat Jenderal Perencanaan Pertahanan, Direktorat Jenderal Potensi Pertahananan, Direktorat Jenderal Kekuatan Pertahanan; (4) Eselon Pendukung yang terdiri dari Badan Sarana

[46] Sumber: Pusat Kodifikasi Kementerian Pertahanan, 2011, <http://ncb45.or.id/index.php?mod=content&cmd=loadcontent&id=19>, diakses pada 28 Desember 2014.

[47] Diolah oleh Peneliti dari Edaran Peraturan Menteri Pertahanan Nomor 16 Tahun 2010.

Pertahanan, Badan Penelitian dan Pengembangan, Badan Pendidikan dan Pelatihan, Pusat Data dan Informasi, Pusat Keuangan, Pusat Komunikasi Publik, Pusat Rehabilitasi Cacat, (5) Eselon Pelaksana Daerah yang dilaksanakan oleh Pelaksana Tugas Pokok Kementerian Pertahanan di daerah. Selain memiliki pembagian kerja secara internal, Kementerian Pertahanan juga memiliki hubungan kelembagaan yang bersifat koordinatif tanpa garis komando khusus dengan Markas Besar TNI (Mabes TNI) yang di dalamnya terdapat 19 satuan kerja seperti Pasukan Pengaman Presiden (Paspampres), Badan Intelijen Strategis (BAIS). Selain itu juga memiliki hubungan kelembagaan dengan Markas Besar tiap-tiap angkatan yang ada di Indonesia seperti Angkatan Darat, Angkatan Laut dan Angkatan Darat.[48]

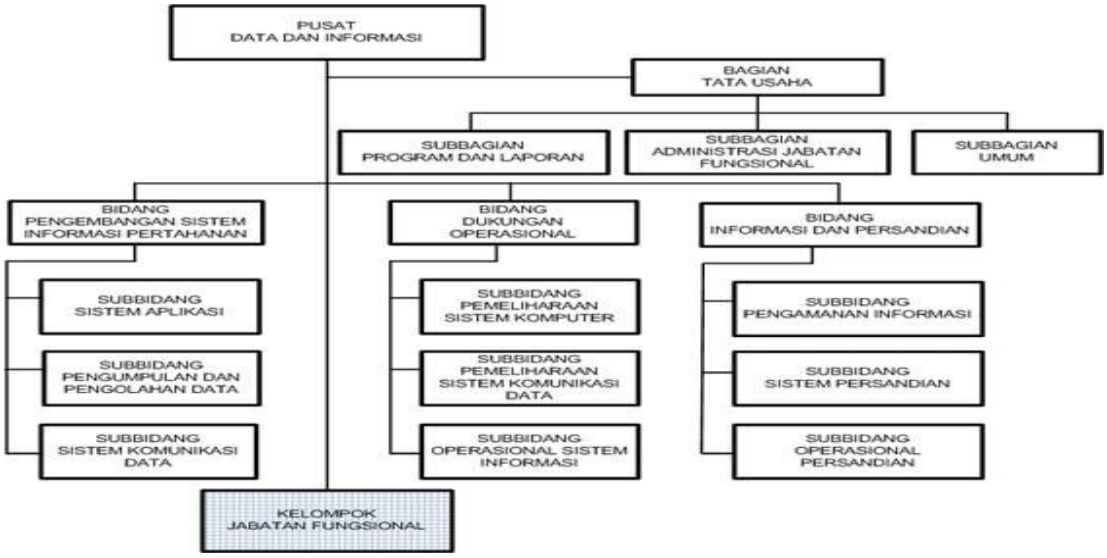
Dari kelima eselon tersebut, dua cabang institusi yang berhubungan langsung dengan pengaturan dan implementasi terhadap pola keterbukaan informasi pertahanan di Indonesia. Kedua cabang unit kerja tersebut adalah Pusat data dan Informasi dan Pusat Komunikasi Publik. Pusat Data dan Informasi bertugas untuk melaksanakan pembinaan, pengembangan dan standarisasi teknis di bidang sistem informasi, teknologi informasi, sistem komunikasi data dan persandian pertahanan negara. Selain satuan kerja yang menangani masalah teknis, pada tataran implementatif, keterbukaan informasi dijamin oleh adanya Pusat Komunikasi Publik yang menjalankan sebagian tugas pokok Kementerian di bidang informasi penyelenggaraan pertahanan negara.

4.1.3.1. Pusat Data dan Informasi

Pusat Data dan Informasi menurut Peraturan Kementerian Pertahanan No.16 Tahun 2010 yang diundangkan di Jakarta pada tanggal 27 September 2010 tentang Organisasi dan Tata Kerja Kementerian Pertahanan Pasal 1149 merupakan eselon pendukung di Kementerian Pertahanan yang

[48] Wawancara dengan Sekretaris Jenderal Kementerian Pertahanan pada 24 November 2014 pukul 15.30 WIB di Kementerian Pertahanan, Jakarta Pusat.

menyelenggarakan fungsi; (1) Perumusan dan pelaksanaan kebijakan teknis di bidang pembinaan data dan informasi pertahanan; (2) Penyusunan standar, norma, pedoman, kriteria dan prosedur di bidang pengembangan sistem, dukungan teknis operasional, persandian dan administrasi serta teknologi informasi pertahanan; (3) Pelaksanaan dan evaluasi kebijakan teknis di bidang pengembangan sistem, dukungan teknis operasional, persandian dan administrasi serta teknologi informasi pertahanan; (4) Pelaksanaan bimbingan dan supervisi teknis di bidang pengembangan sistem, dukungan teknis operasional, persandian dan administrasi serta teknologi informasi pertahanan; (5) Penyiapan bahan administrasi pembinaan sumber daya manusia pranata komputer dan persandian; dan (6) Penyiapan bahan perencanaan program dan anggaran, evaluasi dan laporan, pembinaan kepegawaian, data dan informasi, dokumentasi, kepustakaan, ketatalaksanaan dan kelembagaan serta ketatausahaan dan kerumahtanggaan.



Gambar 4.6. Struktur Organisasi Pusat Data dan Informasi[49]

[49] Sumber: Pusat Data dan Informasi Kementerian Pertahanan, *Struktur Organisasi Pusdatin Kemhan (online),* <http://pusdatin.kemhan.go.id/?pg=142>*,* diakses pada 28 Desember 2014.

Berdasarkan gambar 4.6. mengenai uraian tugas, fungsi dan struktur kerja yang dimiliki oleh Pusat Data dan Informasi memiliki peran yang sangat penting dalam menjamin keamanan informasi pertahanan yang dimiliki Kementerian Pertahanan. Karena hal tersebut, peneliti menilai bahwa Pusat Data dan Informasi memegang kunci dari berjalan atau tidaknya pola keterbukaan informasi pertahanan yang tepat secara teknis.

4.1.3.2. Pusat Komunikasi Publik

Pusat Komunikasi Publik merupakan unit kerja di dalam Kementerian Pertahanan yang berperan sebagai Pejabat Pengelola Informasi dan Dokumentasi. Menurut Peraturan Menteri Pertahanan No.16 Tahun 2010 tentang Organisasi dan Tata Kerja Kementerian Pertahanan mengenai Pusat Komunikasi Publik merupakan salah satu unit eselon pendukung di Kementerian Pertahanan yang menyelenggarakan fungsi; (1) Perumusan dan pelaksanaan kebijakan teknis di bidang informasi pertahanan; (2) Penyusunan standar, norma, pedoman, kriteria dan prosedur di bidang pemberitaan , opini dan kerjasama informasi pertahanan; (3) Pelaksanaan dan evaluasi kebijakan teknis di bidang pemberitaan, opini dan kerjasama informasi pertahanan; (4) Pelaksanaan bimbingan dan supervisi teknis dan perijinan di bidang pemberitaan, opini dan kerjasama informasi pertahanan; dan (5) Penyiapan bahan perencanaan program dan anggaran, evaluasi dan laporan, pembinaan kepegawaian, data dan informasi, dokumentasi, kepustakaan, ketatalaksanaan dan kelembagaan serta ketatausahaan dan kerumahtanggaan Pusat. Secara singkat dapat dinyatakan bahwa Pusat Komunikasi Publik memiliki tugas utama sebagai unit yang melakukan penyebarluasan informasi bidang pertahanan. Pada tingkatan yang lebih spesifik, Pusat Komunikasi Publik terdiri atas beberapa sub bidang[50] yaitu;

[50] Wawancara dengan Kepala Sub Bidang Informasi, Pusat Komunikasi Publik Kementerian Pertahanan pada 5 Februari 2015 pukul 09.30 WIB di Kantor Pusat Komunikasi Publik Kementerian Pertahanan, Jakarta Pusat.

(1) Pemberitaan yang terdiri dari bagian Peliputan dan Publikasi. Bagian ini memiliki tugas untuk mempersiapkan keperluan dalam kegiatan konferensi pers, memberikan informasi mengenai peristiwa dan kegiatan yang terjadi di dalam maupun di luar lingkungan Kementerian Pertahanan melalui berita, membuat himbauan kepada seluruh pegawai Kementerian Pertahanan, menyiapkan data dan informasi selengkap-lengkapnya guna memudahkan komunikasi Kementerian Pertahanan dan media massa;

(2) Pengelolaan Opini Publik yang terdiri dari Penyiapan Opini, Pembentukan Opini, dan *Cyber Media*. Bagian ini memiliki tugas khusus untuk memantau berita dari media massa dan media sosial, membuat kumpulan berita dari berbagai media yang berkaitan dengan Kementerian Pertahanan, melakukan pencarian fakta-fakta dan data pendukung serta melakukan klarifikasi dari berita yang ada dari sumber eksternal dalam rangka pencitraan. Salah satu tugas yang dilakukan melalui *cyber media* adalah *image building operations* yang merupakan satuan khusus untuk meningkatkan citra Kementerian Pertahanan di dalam masyarakat menggunakan sosial media seperti *twitter* dan *facebook.* Selain juga menerima opini dan masukan dari publik yang dapat menjadi nilai membangun untuk meningkatkan kualitas kinerja, mengubah pola pikir, sikap dan tindakan, mengubah budaya kerja serta menegakkan etika di lingkungan Kementerian Pertahanan;

(3) Kerjasama informasi yang terdiri dari Kerjasama Kelembagaan, Penerbitan, dan Informasi. Bagian ini memiliki tugas yang bersifat ekternal dan internal. Secara internal, bagian ini bertugas menyusun pesan kunci dalam bentuk amanat pimpinan, selain itu juga secara aktif bertugas untuk mengumpulkan informasi dari satuan kerja di Kementerian Pertahanan seperti Strahan, Renhan, Kuathan, Pothan, dan Ranahan. Sedangkan tugas eksternal termasuk untuk

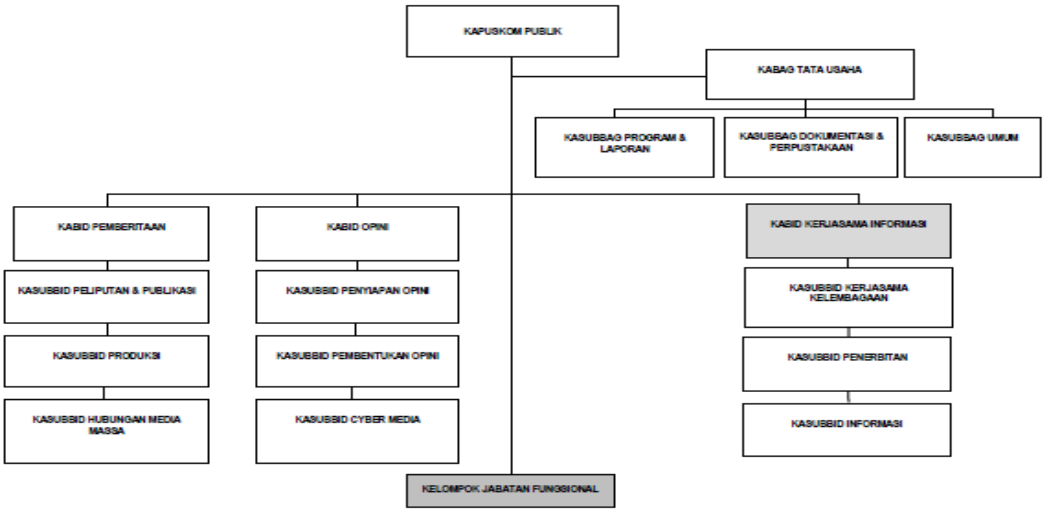
membangun kerjasama antar lembaga dan instansi, serta menyebarkan informasi kepada lembaga dan institusi lain. Bagian ini pula yang bertanggungjawab mendampingi Kepala Pusat Komunikasi Publik untuk berhubungan dengan komisi I Dewan Perwakilan Rakyat Republik Indonesia.

Dalam melakukan tugasnya melalui sub-sub bidang tersebut, Pusat Komunikasi Publik melaksanakan penyebarluasan informasi pertahanan yang dilakukan melalui media meliputi media cetak, media elektronik, dan media *on-line.* Untuk melakukan tugas penyebarluasan informasi pertahanan ini dilakukan melalui beberapa cara, yaitu;

(1) Penyebaran informasi pertahanan melalui pengumuman yang meliputi seluruh informasi pertahanan yang berada pada Kemhan selain Informasi Yang Dikecualikan dapat diakses oleh publik melalui situs Kementerian Pertahanan (www.kemhan.go.id) dan melalui Permohonan Informasi Pertahanan. Selain itu juga informasi pertahanan yang wajib disediakan dan diumumkan secara berkala, diumumkan melalui situs Kementerian Pertahanan (www.kemhan.go.id) dan media cetak yang tersedia.

(2) Penyebarluasan informasi pertahanan melalui permintaan, yaitu Informasi pertahanan yang wajib tersedia setiap saat disediakan oleh Kementerian Pertahanan melalui Pusat Komunikasi Publik.

Untuk menyelenggarakan penyebarluasan informasi pertahanan dapat menggunakan media komunikasi, seperti media massa berupa surat kabar, majalah, radio dan televisi sekurangkurangnya satu bulan sekali. Selain itu diselenggarakan pula melalui situs Kementerian Pertahanan (www.kemhan.go.id) sekurang-kurangnya setiap hari dilakukan perbaruan pada konten. Media Interpersonal seperti sarasehan, ceramah, diskusi, lokakarya sekurang-kurangnya setiap tahun sekali. Selain itu juga melalui media luar ruang berupa, media buletin, *leaflet*, *booklet*, brosur, *newsletter*, spanduk, dan baliho dilakukan didasarkan pada kebutuhan.



Gambar 4.7. Struktur Organisasi Pusat Komunikasi Publik[51]

4.2. Analisis Data dan Hasil Temuan

Dalam sub bab ini peneliti akan menguraikan secara singkat mengenai identifikasi permasalahan yang dialami oleh sistem yang saat ini telah berjalan dan pemecahan masalah melalui kebijakan dan sistem yang telah diterapkan baik melalui peran Kementerian Komunikasi dan Informatika maupun Kementerian Pertahanan.

4.2.1. Analisis Interpretasi naratif (*Narrative Interpretative Analysis)*

Analisis interpretasi naratif sudah banyak digunakan oleh peneliti yang menggunakan metode kualitiatif dalam penulisannya. Jenis analisis interpretasi naratif ini dikembangkan secara lebih luas oleh Jane Stokes dalam sebuah buku metode riset yang memfokuskan pada penelitian tentang komunikasi, informasi dan media dalam ilmu sosial dan humaniora. Stokes dalam buku yang berjudul *How to Do Media and Cultural Studies* itu memaparkan bahwa pemahaman mengenai suatu sistem atau suatu hal hanya bisa dicapai dari pandangan pelaku realitas tersebut. Dalam penelitian interpretasi naratif ini, semua fenomena dianggap sebagai hasil sebuah

[51] Korespondensi dengan Defense Media Center Kementerian Pertahanan pada 5 Februari 2015.

konstruksi sosial sehingga hasil penelitian menjadi sumber yang sangat relevan dan bermanfaat dalam analisis.[52] Dalam tesis ini data tersebut didapatkan dari artifak wawancara termasuk dari transkrip wawancara dan korespondensi yang dilakukan dengan narasumber.

4.2.2 Permasalahan Pola Keterbukaan Informasi bidang Pertahanan

Dalam melihat permasalahan yang dialami oleh pola keterbukaan informasi bidang pertahanan di Indonesia secara khusus, perlu meninjau mengenai kondisi sistem keamanan informasi di Indonesia baik pada tingkatan masyarakat maupun tingkatan pemerintah sebagai sebuah entitas negara. Beberapa data yang dimiliki oleh Kementerian Komunikasi dan Informatika menunjukkan bahwa saat ini Indonesia merupakan negara yang memiliki pelanggan telepon selular sebanyak 220 Juta dengan pengguna terhubung pada jaringan internet sebanyak 74,6 Juta koneksi pada tahun 2013 dibandingkan dengan 2,3 Milyar koneksi yang terdapat di dunia. Selain itu, dari yang terhubung dengan jaringan internet tersebut terdapat 43 Juta pengguna situs media sosial Facebook atau pengguna terbanyak kedua di dunia dan 19,5 Juta pengguna situs media sosial Twitter atau pengguna terbanyak keenam di dunia .[53]

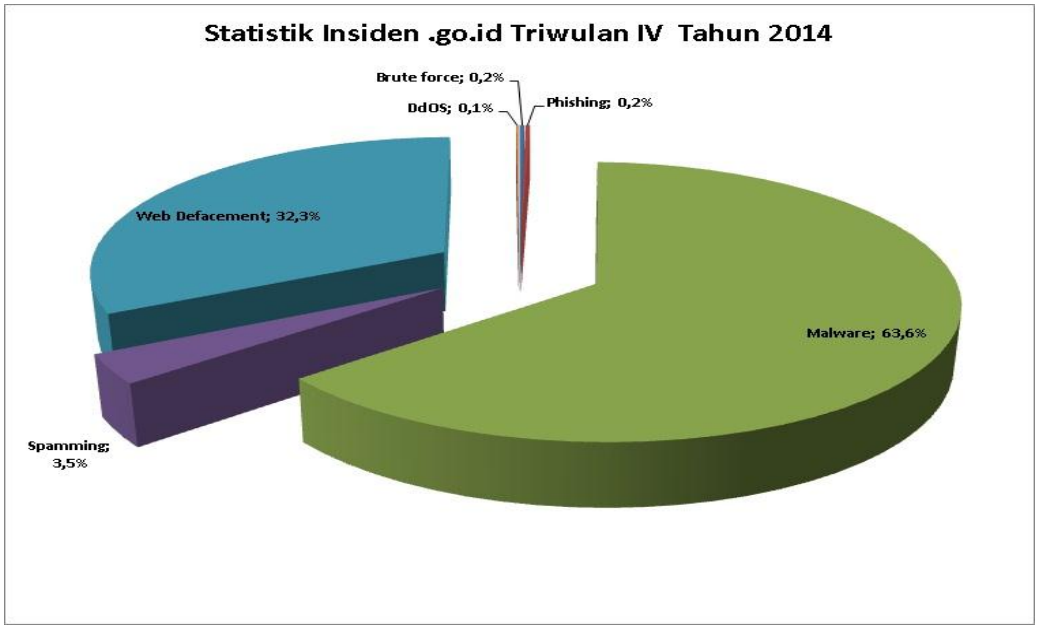
Kondisi pengguna tersebut juga ditunjang dengan data serangan yang dimiliki oleh Kementerian Komunikasi dan Informasi pada tahun 2013 saja jumlah insiden serangan di ruang siber yang terjadi di dunia mencapai satu juta insiden, dan cenderung meningkat tiap harinya. Khusus serangan yang terjadi di Indonesia disebabkan kelemahan sistem dan aplikasi yang telah diketahui (*common vulnerability*). Situs *domain* milik Institusi pemerintah di Indonesia termasuk paling banyak mengalami serangan dan paling banyak

---

[52] J. Stokes, *How to Do Media and Cultural Studies,* edisi Bahasa Indonesia, *Panduan untuk Melaksanakan Penelitian dalam Kajian Media dan Budaya,* diterjemahkan oleh Santi Indra Astuti, Bentang Pustaka, Yogyakarta, 2007, hal.72.

[53] Paparan Direktur Keamanan Informasi, Kementerian Komunikasi dan Informasi tentang 'Kebijakan Pemerintah Terkait dengan Keamanan Informasi dan Dunia Siber' pada 4 Oktober 2012 di Makassar.

dialami oleh situs-situs milik Pemerintah Daerah di Indonesia. Dapat dilihat melalui gambar 4.8. bahwa dari serangan-serangan tersebut yang paling sering terjadi adalah serangan *malware/malicious code* terutama virus lokal dan *phising, scam* serta *spam* yang juga mulai menyebar ke media yang ada di telepon selular disusul oleh *Web defacing rally* (*vandalism*) dengan teknik eksploitasi database SQL. Selain itu juga masih besarnya keterlibatan aktor asing dalam sistem informasi Indonesia baik dalam bentuk infrastruktur maupun non-infrastruktur membuat informasi yang ditukarkan dalam sistem tersebut sangat rawan keamanannya.[54] Banyaknya kesalahan prosedur pengamanan dan kelalaian pengelola sistem menimbulkan maraknya kebocoran data-data, terutama data penting milik pemerintah.



Gambar 4.8. Statistik Data Serangan ke Situs Institusi Pemerintah[55]

[54] Wawancara dengan Kepala Sub Bidang Pembinaan Fungsi Dinas Informasi dan Pengolahan Data TNI Angkatan Darat pada 23 Januari 2015 pukul 09.30 WIB di Markas Besar TNI Angkatan Darat, Jakarta Pusat.

[55] Sumber: Pusat Monitoring dan Penanganan Insiden Keamanan Informasi Kementerian Komunikasi dan Informatika, *Statistik Insiden Respon Domain .go.id (online),* <http://govcsirt.kominfo.go.id/insiden-defacement-terjadi-di-situs-pemerintahan/>, diakses pada 1 Januari 2015.

Dengan adanya keadaan saat ini yang menunjukkan bahwa sebagian besar masyarakat Indonesia terhubung baik melalui koneksi internet maupun selular, harus disadari pula bahwa regulasi keterbukaan informasi pertahanan yang telah ditetapkan oleh pemerintah Indonesia baik melalui peran Kementerian Komunikasi dan Informatika maupun Kementerian Pertahanan harus diselaraskan dengan sistem keamanan informasi yang baik dan dapat meminimalkan celah yang dimiliki regulasi tersebut. Di tingkat pemerintahan juga harus disadari bahwa makin luasnya aplikasi dan konten menyebabkan hampir semua perundangan di semua sektor pemerintahan saat ini terkait dengan ruang siber. Alasan tersebutlah yang menyebabkan informasi bidang pertahanan dilindungi oleh dua sistem keamanan informasi yaitu sistem keamanan informasi Kementerian Komunikasi dan Informatika dan sistem keamanan milik informasi Kementerian Pertahanan.

Meskipun telah terdapat larangan dan hukuman yang jelas bagi pihak-pihak yang melakukan akses terhadap informasi pertahanan yang dikecualikan, tetapi seiring dengan dinamisnya era peperangan informasi dan masih kurangnya kesadaran berperilaku dan bertindak dalam menghadapi peperangan informasi, masih terdapat peristiwa yang berkenaan dengan keterbukaan informasi pertahanan baik pengelolaan terhadap informasi pertahanan yang dikecualikan maupun tidak dikecualikan yang dianggap mengancam kepentingan nasional Indonesia. Di sisi lain terdapat kontradiksi bahwa ketertarikan masyarakat Indonesia terhadap informasi pertahanan yang diperbolehkan masih sangat sedikit dan cenderung kurang besar jika dibandingkan dengan informasi publik di bidang lain dinilai dari akses terhadap informasi yang disediakan oleh Pusat Komunikasi Publik Kementerian Pertahanan.[56]

Informasi seperti Pengajuan Rancangan Undang-Undang Komponen Cadangan (RUU Komcad) misalnya, yang berkaitan langsung dengan peran

[56] Wawancara dengan Kepala Sub Bidang Informasi, Pusat Komunikasi Publik Kementerian Pertahanan pada 5 Februari 2015 pukul 09.30 WIB di Kantor Pusat Komunikasi Publik Kementerian Pertahanan, Jakarta Pusat.

serta masyarakat Indonesia dalam pertahanan negara. Informasi tersebut ramai diberitakan pada pertengahan tahun 2013 namun kembali tenggelam karena tidak adanya keseriusan dari pihak legislatif dan tidak ada kepedulian yang besar mengenai hal ini dari masyarakat.[57] Selain itu, berita mengenai RUU Komcad ini tidak hanya kurang mendapat dukungan dari masyarakat tetapi juga muncul di berbagai media bahwa RUU Komcad tersebut adalah komoditas politik salah satu pihak pada pemilihan umum 2014 lalu.[58] Hal yang sama terjadi juga dengan Rancangan Undang-Undang Keamanan Nasional (RUU Kamnas), undang-undang yang nantinya akan sangat terikat dengan kegiatan warga negara justru tidak tersosialisasi dengan baik kepada masyarakat dan yang timbul di pemberitaan justru adalah bagaimana terjadi tarik-menarik kepentingan dalam pembuatan RUU Kamnas ini.[59] Di sisi lain, pembahasan mengenai *tank leopard* yang tidak berdampak langsung terhadap masyarakat justru menjadi topik pembicaraan dan pemberitaan dalam masyarakat. Hal ini bahkan mendorong kepada diskusi yang cenderung membagi bangsa Indonesia menjadi kubu berlawanan karena bersamaan dengan adanya pemilihan umum 2014 lalu.[60] Peristiwa tersebut dianggap mengancam bagi kepentingan nasional Indonesia secara umum. Hal itu menandakan mekanisme yang terdapat dalam pola keterbukaan informasi pertahanan Indonesia belum dapat berfungsi secara maksimal dalam mencapai tujuannya.

Selain permasalahan secara umum di tingkat individual dan pemerintahan, Bambang Heru Tjahjono dalam kapasitasnya sebagai Direktur

---

[57] Lihat 'DPR Diminta Serius Bahas RUU Komcad',*Suara Pembaruan,* 3 September 2013, <http://sp.beritasatu.com/home/dpr-diminta-serius-bahas-ruu-komcad/41176>, diakses pada 16 Februari 2015.

[58] Lihat 'Pemerintah Harus Yakinkan Publik Soal Komcad', *Suara Pembaruan,* 12 Juni 2013, <http://sp.beritasatu.com/home/pemerintah-harus-yakinkan-publik-soal-komcad/36900>, diakses pada 16 Februari 2015.

[59] Lihat 'Terancam Kehilangan Kewenangan, Polri Pasrah', *Hukum Online*, 1 Februari 2012, <http://www.hukumonline.com/berita/baca/lt4f294054bf522/terancam-kehilangan-kewenangan-polri-pasrah>, diakses pada 17 Februari 2015.

[60] Lihat 'Prabowo tegaskan Tank Leopard bisa digunakan di RI, Jokowi tidak', *Merdeka.com,* 22 Juni 2014, <http://www.merdeka.com/politik/prabowo-tegaskan-tank-leopard-bisa-digunakan-di-ri-jokowi-tidak.html>, diakses pada 17 Februari 2015.

Keamanan Informasi, Kementerian Komunikasi dan Informatika menyampaikan pula bahwa terdapat faktor-faktor yang masih menjadi hambatan bagi upaya pengamanan yang dilakukan oleh Kementerian Komunikasi dan Informatika, diantaranya;

(1) Lemahnya koordinasi antar lembaga instansi pemerintah mengenai penegakan sistem keamanan informasi.
(2) Implementasi pengamanan sistem keamanan informasi di Indonesia yang tidak berjalan secara simultan sehingga berjalan sesuai dengan institusi masing-masing antara pengamanan pada usaha bisnis swasta, pemerintahan dan individual.
(3) Tingkat kepedulian dan kewaspadaan yang masih rendah mengenai pentingnya data dan informasi baik di tingkat institusional pemerintahan maupun masyarakat Indonesia secara umum. Hal ini berkaitan pula dengan lemahnya integritas yang terdapat pada pegawai institusional dan budaya permisif dan tak acuh pada perilaku masyarakat secara umum.
(4) Tingginya kesenjangan digital di Indonesia yang diakibatkan luasnya wilayah Indonesia.

Di sisi lain, sebagai institusi yang berurusan langsung dengan informasi bidang pertahanan, Kementerian Pertahanan menghadapi hambatan yang berbeda dengan Kementerian Komunikasi dan Informatika dalam menentukan pola keamanan terhadap informasi bidang pertahanan. Menurut Letnan Jenderal Ediwan Prabowo terdapat beberapa faktor yang dianggap masih menghambat sistem keamanan informasi bidang pertahanan secara maksimal. Faktor-faktor tersebut antara lain;

(1) Belum cukupnya infrastruktur teknologi di Indonesia untuk melakukan pengamanan informasi menggunakan pendekatan menyerang meskipun di sisi lain dinyatakan pula untuk pendekatan defensif Indonesia sudah cukup memiliki sistem yang baik.

(2) Belum adanya regulasi yang mengkoordinasikan secara tepat mengenai pengelolaan informasi dan teknologi di lingkungan Kementerian Pertahanan dan TNI yang terkait juga dengan pengelolaan alat-alat yang sensitif dan memiliki kegunaan intelijen.
(3) Terbatasnya anggaran untuk memilih penggunaan alat yang lebih canggih dalam memaksimalkan sistem keamanan informasi.
(4) Alat-alat yang dipakai saat ini untuk menggerakkan sistem keamanan informasi pertahanan sebagian besar masih merupakan buatan dari luar negeri sehingga sistem ini masih memberikan celah kelemahan yang besar.
(5) Sumber daya manusia yang belum cukup mampu dalam hal operasional teknologi yang digunakan sampai pada proses manajemennya. Karena untuk melakukan operasi maupun manajemen terhadap teknologi dan peralatan yang digunakan membutuhkan orang-orang yang terlatih. Untuk mengurangi celah dari kekurangan tersebut, Kementerian Pertahanan telah memberikan pendidikan dan latihan untuk mendidik operator dan kursus manajemen.

4.2.3. Pemecahan Masalah dalam Pola Keterbukaan Informasi bidang Pertahanan

Dalam menangani permasalahan yang muncul baik di tingkat nasional, tingkat kementerian maupun tingkat individual yang menyentuh masyarakat, perlu diberlakukan sistem keamanan informasi bidang pertahanan yang dapat menjadi solusi bagi permasalahan yang telah disampaikan pada bagian sebelumnya. Pemecahan masalah yang diimplementasikan dalam pola keterbukaan informasi bidang pertahanan melalui sistem keamanan informasi baik yang diimplementasikan oleh Kementerian Komunikasi dan Informatika serta Kementerian Pertahanan harus mendasarkan pada tiga

pilar yang saling terkait dalam paradigma informasi yaitu faktor manusia (*people*), proses (*process*), dan teknologi (*technology*).

4.2.3.1 Sistem Keamanan Informasi Pertahanan yang Diterapkan oleh Kementerian Komunikasi dan Informatika

Kementerian Komunikasi dan Informatika saat ini menjadi salah satu kementerian yang giat dalam usaha mewujudkan sistem informasi yang aman bagi informasi milik pemerintah, termasuk di dalamnya informasi yang penting dan vital seperti informasi bidang pertahanan. Dalam penyelenggaraan tata kelola sistem keamanan informasi bidang pertahanan, faktor keamanan merupakan aspek yang sangat penting diperhatikan untuk mewujudkan keamanan informasi yang melingkupi ketiga aspek utama yang menyangkut kerahasiaan, keutuhan dan ketersediaan. Beberapa inisiatif yang diterapkan oleh Kementerian Komunikasi dan Informatika digunakan agar hambatan dan masalah yang muncul dalam pola keterbukaan informasi bidang pertahanan dapat diminimalisasi.

Secara garis besar, Kementerian Komunikasi dan Informatika memiliki beberapa inisiatif yang digunakan sebagai bentuk usaha pengamanan informasi yang didasarkan pada Surat Edaran Menteri Kementerian Komunikasi dan Informatika No. 05/SE/M.KOMINFO/07/2011 tentang Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik, seperti[61]; (1) Program Internet Terpercaya, Sehat dan Aman (TRUST+) yang bertujuan untuk memberikan perlindungan terhadap akses internet dengan berdasarkan pada informasi yang sehat dan terpercaya, selain itu memberikan perlindungan terhadap masyarakat dalam menghadapi nilai, etika, moral dan kaidah yang tidak sesuai dengan budaya Bangsa Indonesia, serta melakukan penghematan terhadap penggunaan akses internet (*internet utilization*) di Indonesia; (2) Program Kampanye Nasional

[61] Paparan Direktur Keamanan Informasi, Kementerian Komunikasi dan Informasi tentang Kondisi Keamanan Informasi di Indonesia pada 13 Mei 2013 di STIKOM, Bali.

Sadar Keamanan Informasi (Go Data) yang merupakan gerakan kepedulian terhadap data yang bertujuan untuk menghimbau dan mengingatkan agar masyarakat selalu terjaga dan sadar terhadap data-data pribadi yang dimiliki; (3) Program untuk menyaring dan memperketat akses ke situs atau konten yang dianggap ilegal dalam Undang-Undang yang bertujuan untuk melindungi kepentingan umum dari konten internet yang berpotensi memberikan dampak negatif atau merugikan; (4) Implentasi Indeks KAMI yang merupakan aplikasi yang digunakan sebagai alat bantu untuk menganalisis dan mengevaluasi tingkat kematangan penerapan keamanan informasi di sebuah institusi yang didasarkan pada kesesuaian dengan kriteria SNI ISO/IEC 27001 sebagai standar manajemen keamanan sistem informasi. Tiap-tiap program memiliki cara kerja dan fungsi yang berbeda namun semua program tersebut memiliki tujuan besar yang sama, yaitu mengantarkan Indonesia pada keamanan informasi yang lebih baik lagi.

Program pertama yang dilakukan sebagai salah satu upaya menegakkan sistem keamanan informasi, termasuk informasi pertahanan adalah TRUST+. TRUST+ merupakan arsitektur jaringan terkonvergen yang berfungsi sebagai penyaring situs-situs yang dapat diakses. Oleh Kementerian Komunikasi dan Informatika, TRUST+ digunakan untuk menghalau situs-situs yang masuk kategori berisikan konten negatif. Beberapa indikator yang digunakan oleh arsitektur tersebut antara lain adalah situs yang mengandung atau menawarkan konten pornografi, terorisme, dan hal negatif lainnya. Dalam kampanye yang dilakukan melalui TRUST+ penekanan dilakukan agar masyarakat dapat secara aktif sadar dan berpartisipasi untuk membedakan antara situs atau konten yang negatif dan konten yang positif. Kampanye ini dilengkapi juga dengan sistem pengaduan agar masyarakat dapat melaporkan informasi tentang situs atau konten.[62] Situs atau konten tersebut dibagi dalam dua jenis kategori yaitu ‘Daftar Putih’

[62] Tentang TRUST+ diakses dari http://trustpositif.kominfo.go.id/ , diakses pada 2 Januari 2015.

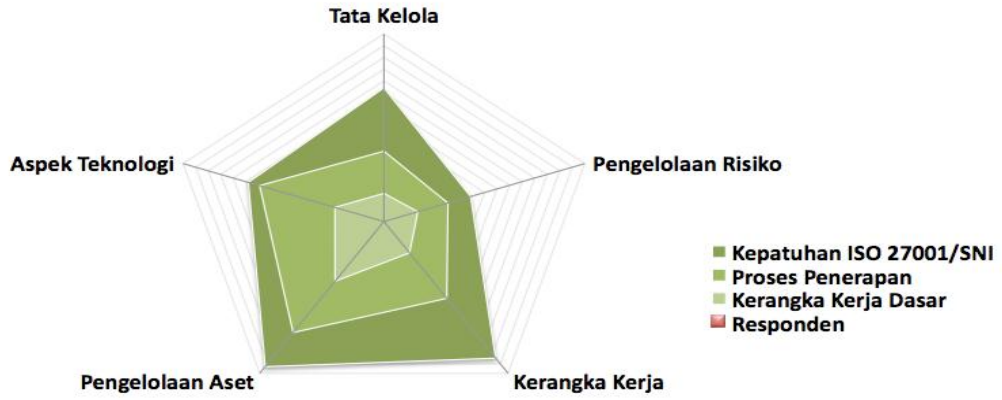
yang berarti *domain* kategori tersebut bersifat positif dan terpercaya, misalnya situs milik pemerintah. Kategori kedua adalah ‘Daftar Hitam’ yang berarti *domain* tersebut harus disaring karena berisi konten negatif, misalnya konten pornografi.

Program kedua yang dilakukan oleh Kementerian Komunikasi dan Informatika sebagai bentuk pengamanan informasi adalah mengampanyekan program Go Data. Go Data adalah gerakan kepedulian terhadap data, dimana gerakan ini bertujuan menghimbau dan menyebarkan kewaspadaan seluas-luasnya agar masyarakat Indonesia lebih sadar untuk berhati-hati dalam melakukan berbagi informasi pribadi melalui media siber. Dengan meluasnya era digital dan dampak globalisasi, Kementerian Komunikasi dan Informasi menganggap bahwa masyarakat Indonesia belum banyak menyadari penting dan rawannya data berbentuk digital untuk disalahgunakan oleh banyak pihak. Kampanye ini merupakan salah satu dari keseluruhan tata kelola keamanan informasi yang dilakukan Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika.

Program ketiga yang dilakukan yaitu untuk menyaring situs dan konten ilegal juga dibantu oleh program TRUST+. Program TRUST+ yang digunakan menekankan pada fungsinya yang dapat membuat situs-situs yang menawarkan konten ilegal tidak dapat diakses oleh pengguna internet di Indonesia. Dalam menjalankan fungsi ini, terdapat tim yang menangani *control* dan *monitoring center*. Tim inilah yang bertugas untuk menemukan situs-situs yang berpotensi mengandung konten negatif yang selanjutnya akan dimasukkan ke dalam daftar hitam. Di samping itu, tim tersebut juga bertugas untuk melakukan analisis profil terhadap situs-situs yang beredar di Indonesia untuk menentukan kategorinya semisal pornografi, media sosial, forum, jual-beli, dan lain-lain.

Program keempat yaitu aplikasi yang digunakan untuk menganalisis dan mengevaluasi penerapan keamanan informasi pada institusi-institusi yang menyelenggarakan pelayanan publik. Indeks KAMI (Keamanan

Informasi) berfungsi sebagai indikator penerapan keamanan informasi yang berlaku secara nasional. Kementerian Komunikasi melalui Direktorat Keamanan Informasi terutama Dirjen Aplikasi Informatika melakukan pembinaan kepada penyelenggara sistem elektronik layanan publik, salah satunya dengan mengimplementasikan aplikasi Indeks KAMI yang disiapkan oleh Kementerian Komunikasi dan Informatika.



Gambar 4.9. Skema Indeks Keamanan Informasi (Indeks KAMI)[63]

Dengan adanya Indeks KAMI sesuai dengan gambar 4.9., tiap-tiap kementerian dapat melakukan penilaian mandiri (*self-assessment*) terhadap sistem keamanan informasinya sendiri dengan menggunakan alat bantu indeks tersebut. Pada Indeks KAMI tersebut terdapat beberapa poin indikator yang dipenuhi, yaitu menyangkut; (1) Sistem Manajemen Keamanan Infomasi (SMKI)[64] milik institusi yang melingkupi kerangka kerja, proses, dan dokumentasi; (2) Tanggung jawab manajemen terhadap sistem tersebut; (3) Audit Internal SMKI; (4) Manajemen melakukan peninjauan ulang terhadap SMKI; (5) Peningkatan yang dapat berkelanjutan. Meski begitu, Indeks KAMI ini tidak ditujukan untuk menganalisis kelayakan atau efektivitas sistem

[63] Paparan Kepala Sub Direktorat Budaya Keamanan Informasi, Kementerian Komunikasi dan Informatika tentang Peningkatan Keamanan Informasi Layanan Publik Melalui Indeks Keamanan Informasi pada 1 Desember 2014 di Jakarta.

[64] Sistem Manajemen Keamanan Informasi adalah bagian dari sistem manajemen secara keseluruhan berdasarkan pendekatan resiko bisnis untuk menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, meningkatkan dan memelihara keamanan informasi.

keamanan yang ada, melainkan sebagai perangkat untuk memberikan kondisi kesiapan kerangka kerja keamanan informasi pada pimpinan instansi publik tersebut.

4.2.3.2. Sistem Keamanan Informasi Pertahanan yang Diterapkan pada Kementerian Pertahanan

Dalam sebuah sistem keamanan sebuah informasi, institusi-institusi yang dinyatakan bahwa informasi yang berasal dari kementeriannya adalah informasi yang dikecualikan memiliki sistem keamanan yang lebih ketat dibandingkan dengan kementerian yang tidak memiliki status informasi yang dikecualikan. Kementerian Pertahanan sebagai salah satu institusi yang informasinya tergolong sebagai informasi dikecualikan juga memiliki beberapa program yang diterapkan sebagai usaha mengamankan informasi bidang pertahanan. Hal ini didorong juga dengan fakta bahwa saat ini informasi bidang pertahanan yang digolongkan sebagai informasi yang dikecualikan pun tidak aman dari tersebarnya informasi tersebut. Diantara berbagai alasan yang dapat muncul, misalnya kemungkinan bahwa jika informasi pertahanan yang dikecualikan diinformasikan pada pihak yang tidak memiliki otorisasi oleh pihak yang sebelumnya memiliki otorisasi namun otoritas tersebut sudah tidak lagi melekat pada dirinya.[65] Hal tersebut contohnya terjadi pada salah satu Pusat Penerangan Angkatan yang melakukan wawancara dengan media massa tentang pengadaan senjata meskipun otoritas tersebut tidak lagi dimiliki olehnya.

Menghadapi hal tersebut, saat ini Kementerian Pertahanan telah memiliki sebuah produk perundangan yang dikhususkan untuk mengatur mengenai keamanan informasi pertahanan di kalangan Kementerian Pertahanan yaitu melalui Peraturan Menteri Pertahanan Nomor 68 tahun 2014 tentang Pengamanan Informasi di Lingkungan Kementerian Pertahanan dan Tentara Nasional Indonesia. Peraturan Menteri tersebut diundangkan

[65] Korespondensi dengan Kepala Sub Bidang Pembinaan Fungsi Dinas Informasi dan Pengolahan Data TNI Angkatan Darat pada Januari 2015.

pada tanggal 17 Oktober 2014 yang menandakan semakin sadarnya pemerintah akan kerugian yang dapat timbul dari penguasaan informasi melalui aplikasi yang saat ini menyaru sebagai layanan umum namun ternyata menggunakan ekosistem asing dan infrastruktur asing. Ketika aset informasi nasional ini sudah dikuasai maka menguasai sumber daya milik sendiri pun akan menjadi hal yang sangat sulit.[66]

Dalam menerapkan sistem keamanan informasi bidang pertahanan di lingkungan Kementerian Pertahanan maupun di TNI, melalui Peraturan Menteri Pertahanan Nomor 68 tahun 2014 pun berdasar dari Standar Nasional Indonesia tentang keamanan Informasi yang ditetapkan oleh Kementerian Komunikasi dan Informatika. Untuk menjalankan sistem keamanan informasi bidang pertahanan sesuai dengan peraturan menteri tersebut, Menteri Kementerian Pertahanan membentuk tim keamanan informasi Kementerian Pertahanan yang diketuai oleh Sekretaris Jenderal Kementerian Pertahanan sedangkan Panglima TNI membentuk tim keamanan informasi di lingkungan TNI. Tim ini dibentuk untuk menjaga kerahasiaan dari sifat informasi yang dilindungi dan tidak disediakan untuk dibuka bagi perorangan, lembaga, atau proses yang tidak berwenang. Meski begitu, dinyatakan oleh Sekretaris Jenderal Kementerian Pertahanan, Letnan Jenderal Ediwan Prabowo bahwa sistem yang diberlakukan oleh Kementerian Pertahanan dan TNI untuk saat ini hanya akan bersifat defensif dan belum akan menggunakan pendekatan menyerang.

Implementasi terhadap keamanan informasi yang diterapkan untuk mengamankan informasi difokuskan pada tiga faktor yaitu; (1) Faktor manusia (*people)*, (2) Faktor proses (*process),* (3) Faktor Teknologi. Diterangkan bahwa untuk mengamankan informasi pertahanan agar terjadi minimalisasi kesalahan pada faktor manusia, Kementerian Pertahanan dan TNI menerapkan regulasi pengamanan berikut;

[66] Wawancara dengan Kepala Sub Bidang Pembinaan Fungsi Dinas Informasi dan Pengolahan Data TNI Angkatan Darat pada 23 Januari 2015 pukul 09.30 WIB di Markas Besar TNI Angkatan Darat, Jakarta Pusat.

(1) Pembatasan terhadap seluruh akses pengamanan informasi, termasuk akses masuk ke dalam sistem (*Log on)* dan sistem sandi (*password).*
(2) Pengamanan informasi tersebut dikelola untuk menjamin agar hanya orang dan peralatan yang telah diberi otoritas yang dapat terkoneksi pada jaringan.
(3) Setiap orang yang memiliki otoritas untuk melakukan akses wajib melakukan koordinasi dengan pimpinan tim keamanan informasi yang telah ditugaskan sehingga dapat diambil langkah-langkah keamanan yang diperlukan.

Sedangkan pada faktor proses Kementerian Pertahanan dan TNI menerapkan regulasi pengamanan berikut;

(1) Semua informasi yang berklasifikasi rahasia yang berasal dari satuan kerja harus melalui proses penyandian atau enkripsi yang bekerjasama dengan Lembaga Sandi Negara[67] pada saat melakukan transfer data dan penyimpanannya dengan metode tertentu.
(2) Setiap satuan kerja di lingkungan Kementerian Pertahanan dan TNI menerapkan kegiatan pencadangan data (*back up)* secara berkala sesuai dengan metode standar keamanan informasi dan diletakkan pada tempat yang berbeda.
(3) Penerapan pengamanan informasi ini akan dikaji ulang setiap tahun untuk menjamin efektivitas pelaksanaannya.

Di sisi lain, pada faktor teknologi Kementerian Pertahanan dan TNI menerapkan regulasi pengamanan berikut;

(1) Akses ke dalam sistem informasi di lingkungan Kementerian Pertahanan dan TNI harus dipisahkan antara jaringan internal

[67] Wawancara dengan Sekretaris Jenderal Kementerian Pertahanan pada 24 November 2014 pukul 15.30 WIB di Kementerian Pertahanan, Jakarta Pusat.

dengan eksternal atas persetujuan dari pimpinan tim keamanan informasi.

(2) Akses jaringan nirkabel yang terhubung dengan jaringan internal (*Local Area Network*) harus dibatasi hanya pada pihak yang berwenang atau memiliki otoritas dan mendapat persetujuan dari pimpinan tim keamanan informasi.

4.3 Pembahasan

Berdasarkan hasil penelitian yang diperoleh baik berupa data-data primer maupun sekunder, peneliti akan membahas tentang temuan-temuan yang dihadapkan kepada landasan teori seperti yang dicantumkan dalam Bab 2, yaitu Teori Keunggulan Informasi dan Teori Partisipasi Masyarakat. Teori-teori tersebut dipilih sebagai dasar tujuan yang akan dicapai dalam pola keterbukaan informasi bidang pertahanan yang ideal. Temuan-temuan tersebut nantinya akan digunakan sebagai bahan dalam penyusunan rekomendasi teoritis maupun praktis.

4.3.1. Aspek Tindakan dalam Keunggulan Informasi

Dalam meninjau pola keterbukaan informasi, terutama informasi bidang pertahanan, keunggulan informasi menjadi salah satu tujuan yang ingin dicapai oleh entitas manapun yang menghadapi ancaman non-tradisional berupa peperangan informasi. Pada bab sebelumnya telah dijelaskan bahwa Dorothy Denning menjelaskan bahwa untuk mendapatkan keunggulan informasi, suatu institusi harus menggunakan berbagai teknik dalam peperangan informasi termasuk dalam bentuk propaganda dan teknik pengumpulan intelijen secara tradisional. Selain itu telah dijelaskan pula bahwa keunggulan informasi diartikan sebagai kemampuan suatu institusi untuk mengumpulkan, memproses dan menyebarkan informasi tanpa gangguan dari pihak lawan sementara memanfaatkan kemampuan tersebut untuk menangkal gangguan aliran informasi dari lawan dengan menghalau

pengumpulan, proses dan penyebaran informasi milik lawan. Definisi yang ditulis tersebut tidak bersifat mutlak. Pernyataan tersebut berarti bahwa untuk mendapatkan keunggulan informasi, setiap negara dapat menyesuaikan aksi yang dilakukannya untuk mencapai keunggulan informasi sesuai dengan pendekatan dan doktrin yang digunakan negara tersebut.

Dua pendekatan yang biasa dipakai dalam mencapai keunggulan informasi adalah pendekatan ofensif dan defensif. Jika pendekatan yang digunakan suatu negara adalah pendekatan yang ofensif berarti yang akan dilakukan negara tersebut adalah berusaha untuk menurunkan atau mengeksploitasi kepemilikan dan penggunaan informasi yang dimiliki oleh lawan dan hal tersebut akan dilakukan baik menggunakan cara yang tradisional ataupun cara nontradisional seperti usaha intrusi elektronik ke dalam sistem informasi dan jaringan kontrol milik lawan. Pendekatan yang ofensif juga percaya akan melakukan teknik apapun untuk meyakinkan, menipu, yang dapat membuat pengambil kebijakan dari pihak lawan mendapatkan informasi yang salah. Berbeda dengan pendekatan ofensif, menurut teori keunggulan informasi, pada negara yang digunakan suatu negara adalah pendekatan defensif maka yang dilakukan negara tersebut adalah melindungi secara maksimal sistem keamanan informasi yang dimiliki. Selain itu akan memberikan peningkatan kesadaran terhadap anggota yang dimiliki dalam hal komando dan kontrol melalui cara- cara tradisional seperti pengutamaan keamanan infrastruktur fisik dan melakukan enkripsi pada informasi yang dimiliki. Hal tersebut ditunjang juga dengan cara yang lebih tradisional pula yaitu menggunakan perlindungan antivirus dan mengutamakan transmisi data yang aman.

Dari penjelasan mengenai pendekatan-pendekatan yang dapat dilakukan oleh sebuah negara untuk mencapai keunggulan informasi, peneliti menemukan bahwa Indonesia hingga saat ini menggunakan pendekatan defensif dalam pola keterbukaan informasi pertahanan yang dimiliki. Selain karena hal tersebut sesuai dengan pernyataan yang diungkapkan oleh

Sekretaris Jenderal Kementerian Pertahanan, tetapi juga karena hal tersebut tercermin dari program-program yang dilakukan baik oleh Kementerian Komunikasi dan Informatika atau Kementerian Pertahanan.

Dalam lingkungan Kementerian Komunikasi dan Informatika Program Internet Terpercaya, Sehat dan Aman (TRUST+), Program Kampanye Nasional Sadar Keamanan Informasi (Go Data) yang dipromosikan di tingkat individual sebagai pemilik informasi dan pengguna sistem informasi menunjukkan adanya usaha peningkatan kesadaran dari anggota masyarakat. Sedangkan program implementasi Program Indeks KAMI menunjukkan adanya usaha peningkatan kesadaran terhadap institusi-institusi pemerintah, terlebih institusi yang memiliki informasi bidang pertahanan. Program lain seperti program untuk menyaring dan memperketat akses ke situs atau konten yang dianggap ilegal dalam Undang-Undang merupakan usaha untuk menciptakan lingkungan sistem informasi pertahanan transmisi data yang aman.

Pada lingkungan Kementerian Pertahanan dan Mabes TNI program-program yang dilaksanakan sebagai bentuk pencapaian keunggulan informasi juga menunjukkan bahwa Indonesia menggunakan pendekatan defensif. Hal tersebut karena program yang dijalankan masih tergolong tradisional seperti pembatasan terhadap seluruh akses pengamanan informasi, termasuk akses masuk ke dalam sistem (*Log on)* dan sistem sandi (*password)* yang harus dikoordinasikan secara khusus dengan tim keamanan informasi, kerjasama enkripsi dengan Lembaga Sandi Negara terhadap transfer data dan informasi dengan klasifikasi rahasia, penerapan kegiatan pencadangan data (*back up)* secara berkala melalui peletakan di tempat yang berbeda. Di samping itu terlihat pula dari pengamanan infrastruktur yang bersifat teknis melalui pemisahan antara jaringan internal dengan eksternal Kementerian Pertahanan dan Mabes TNI maupun dari pembatasan akses jaringan nirkabel yang terhubung dengan jaringan intrernal (*Local Area Network*).

Penekanan terbesar dalam pendekatan defensif untuk mencapai keunggulan informasi adalah keamanan infrastruktur sehingga serangan yang masuk dari lawan tidak dihadapi menggunakan serangan terhadap lawan tetapi justru memperkuat keamanan infrastruktur internal. Penekanan tersebut yang saat ini belum dapat dicapai oleh sistem keamanan informasi pertahanan milik Indonesia. Meskipun dinyatakan oleh Kementerian Pertahanan melalui Sekretaris Jenderal maupun Pusat Data dan Informasi Kementerian Pertahanan bahwa sistem pengamanan informasi pertahanan yang bersifat defensif sudah baik dan cukup untuk menghalau serangan sampai saat ini. Masih sangat bergantungnya Indonesia pada infrastruktur dan aplikasi sistem komunikasi dan informasi milik asing telah menimbulkan celah kerawanan terhadap keamanan informasi bidang pertahanan. Kemandirian di bidang infrastruktur dan aplikasi sangat dibutuhkan jika Indonesia ingin memiliki pola keterbukaan informasi pertahanan yang aman dan dapat memenuhi nilai-nilai keunggulan informasi.

Faktor lain yang harus dipenuhi oleh untuk mencapai keunggulan informasi adalah dengan melakukan edukasi dan pelatihan untuk menyosialisasikan paradigma baru ketahanan nasional dalam mengamankan informasi pertahanan. Hal ini hendaknya dilakukan secara aktif baik di jajaran aparatur negara termasuk Kementerian Pertahanan dan Mabes TNI. Pelatihan tersebut tidak cukup hanya pada tataran pegawai saja tetapi juga pada tingkatan pengambil kebijakan dan tingkatan eksekutif. Meskipun dinyatakan pula bahwa untuk mengurangi celah dari kekurangan tersebut, Kementerian Pertahanan telah memberikan pendidikan dan latihan untuk mendidik operator dan kursus manajemen keamanan informasi pada pegawai Kementerian Pertahanan dan Mabes TNI.

4.3.2. Aspek Perilaku dalam Partisipasi Masyarakat

Sebagaimana telah disebutkan pada bagian sebelumnya bahwa dengan adanya era globalisasi, terjadi perkembangan teknologi komunikasi

dan informasi yang pesat sehingga membawa dampak yang besar pada pola keamanan informasi di tingkat pemerintah, terutama dengan informasi penting seperti informasi bidang pertahanan. Adanya nilai demokrasi dalam kehidupan bermasyarakat saat ini diiringi dengan semakin dinamisnya perkembangan teknologi komunikasi dan informasi menuntut Indonesia untuk mengambil langkah melalui kebijakan-kebijakan yang diharapkan bersifat solutif sehingga dapat meminimalkan kerawanan terhadap informasi bidang pertahanan yang bersumber baik dari dalam maupun luar negeri.

Dalam teori ini, tujuan yang ingin dicapai melalui partisipasi masyarakat adalah;

(1) Membuat alam demokrasi semakin demokratis. Hal ini dapat dilihat dari program TRUST+ yang diterapkan oleh Kementerian Komunikasi dan Informatika melalui pelibatan masyarakat secara aktif untuk melaporkan situs-situs yang menyebarkan berita yang tidak dapat dipercaya atau konten yang negatif. Meskipun dapat terlihat pula bahwa tujuan ini belum dapat dicapai karena masyarakat Indonesia sebagian besar bersifat permisif dengan tidak memanfaatkan jalur pelaporan yang disediakan oleh pemerintah melalui Kementerian Komunikasi dan Informatika.

(2) Melakukan redefinisi terhadap struktur kekuatan politis. Tujuan yang ingin dicapai melalui partisipasi masyarakat ini belum dapat dicapai dengan sempurna menyadari bahwa salah satu hambatan yang dihadapi saat ini adalah termasuk besarnya kesenjangan digital di Indonesia yang diakibatkan luasnya wilayah Indonesia sehingga infrastruktur yang dimiliki satu wilayah bisa sangat berbeda dengan wilayah lain.

(3) Meningkatkan tingkat kredibilitas dan legitimasi dari masyarakat terhadap pemerintah. Hal ini untuk saat ini menjadi tujuan yang paling mendesak bagi pemerintah Indonesia untuk segera diwujudkan. Keterbukaan informasi pertahanan dengan sistem

yang ada saat ini masih belum dapat mewujudkan tujuan ini karena masih lebih banyak digunakan oleh Lembaga Swadaya Masyarakat dalam mengontrol institusi publik dibanding terbangunnya kesadaran masyarakat untuk dapat menerima informasi yang transparan dari pemerintah.

(4) Menertibkan konflik dan membangun konsensus bersama. Tujuan ini dapat dicapai jika telah terbangun suatu sistem keterbukaan informasi yang dapat berjalan selaras dengan sistem keamanan informasi. Namun hal ini belum dapat dicapai dengan maksimal karena sistem keamanan informasi yang belum didukung dengan infrastruktur sehingga masih sering menciptakan konflik baik di tingkat pemerintahan atau di tingkat individu masyarakat.

(5) Mendorong munculnya opini dan konsultasi dari masyarakat. Tujuan ini sudah diwadahi melalui adanya unit kerja yang mengelola opini publik baik di tingkat Kementerian Komunikasi dan Informatika serta di Kementerian Pertahanan. Namun, keberadaan ini masih belum menunjukkan kinerja yang maksimal karena tidak memiliki produk yang jelas dari pengelolaan opini tersebut.

(6) Meningkatkan akuntabilitas dan transparansi dalam tingkat pemerintahan. Tujuan ini adalah tujuan utama bagi pemerintah dalam membentuk pola keterbukaan informasi di Indonesia. Namun hal tersebut juga masih mengalami hambatan dengan masih banyaknya daerah yang belum memiliki Komisi Informasi Daerah. Di tingkatan eksekutif juga masih terdapat institusi yang belum memiliki Pejabat Pengelola Informasi dan Dokumentasi di institusinya masing-masing. Meskipun keberadaan institusi ini merupakan implementasi dari UU tentang keterbukaan informasi publik.

BAB 5

SIMPULAN DAN SARAN

Tulisan tentang pola keterbukaan informasi pertahanan di Indonesia sebagai ancaman nontradisional yang didasarkan pada Undang-Undang (UU) No. 14 tahun 2008 tentang Keterbukaan Informasi Publik, diselaraskan dengan teori Keunggulan Informasi (*Information Supremacy*) dan teori Partisipasi Masyarakat. Pola keterbukaan informasi pertahanan yang saat ini diimplementasikan diharapkan dapat ditingkatkan untuk keberlanjutan keterbukaan informasi pertahanan yang baik.

5.1 Simpulan

Berikut merupakan kesimpulan-kesimpulan yang dihasilkan dari analisis pola keterbukaan informasi bidang pertahanan di Indonesia sebagai ancaman nontradisional.

1. Dalam menentukan pola keterbukaan informasi bidang pertahanan, Indonesia menentukan bahwa hal tersebut diatur oleh dua kementerian utama. Kementerian yang bertanggungjawab terhadap keamanan informasi pertahanan adalah Kementerian Komunikasi dan Informatika sebagai kementerian yang secara umum mengatur tata kelola berbagai informasi publik beserta dengan Kementerian Pertahanan yang secara khusus mengatur tata kelola informasi pertahanan.Sedangkan untuk menentukan regulasi dan sistem keamanan tiap informasi yang dimiliki oleh institusi di Indonesia, Kementerian Komunikasi dan Informatika menjadi kementerian yang berperan sangat penting untuk menjamin tersedianya informasi publik, termasuk di dalamnya informasi bidang pertahanan, yang dibutuhkan oleh masyarakat sebagai bentuk pengawasan terhadap pemerintahan yang baik. Di sisi lain, Kementerian Komunikasi dan

Informatika juga bertanggungjawab untuk menjamin bahwa informasi publik yang tidak seharusnya diketahui publik aman dari pihak yang tidak memiliki otorisasi untuk mengetahuinya melalui sistem keamanan informasi. Di sisi lain, untuk menangani keamanan informasi bidang pertahanan, Kementerian Komunikasi dan Informatika melakukan koordinasi dengan Kementerian Pertahanan sebagai pelaksana fungsi pemerintah di bidang pertahanan, baik pertahanan militer maupun nirmiliter. Pada tingkatan implementatif, kedua kementerian tersebut bekerjasama dengan institusi eksternal Komisi Informasi Pusat sebagai institusi penjamin keterbukaan informasi, termasuk informasi pertahanan beserta dengan Lembaga Sandi Negara yang secara teknis melakukan proses enkripsi.

2. Berdasarkan pertimbangan terbatasnya anggaran, alat dan infrastruktur yang masih tergantung pada buatan luar negeri, serta sumber daya manusia yang belum cukup mampu dalam hal operasional teknologi maupun manajemen teknologi tersebut, dinyatakan oleh Sekretaris Jenderal Kementerian Pertahanan bahwa pola keamanan informasi pertahanan untuk berjalan selaras dengan pola keterbukaan informasi pertahanan adalah dalam pola pendekatan defensif. Dalam pola pendekatan defensif sesuai dengan teori Keunggulan Informasi akan ditandai dengan perlindungan secara maksimal atas informasi yang dimiliki. Selain itu akan memberikan peningkatan kesadaran terhadap anggota yang dimiliki dalam hal komando dan kontrol melalui cara- cara tradisional seperti pengutamaan keamanan infrastruktur fisik dan melakukan enkripsi pada informasi yang dimiliki. Hal tersebut ditunjang juga dengan cara yang lebih tradisional pula yaitu menggunakan perlindungan antivirus dan mengutamakan transmisi data yang aman. Dari indikator yang terdapat dalam teori tersebut, terbukti bahwa Indonesia menggunakan pola pendekatan defensif. Dinyatakan oleh Sekretaris Jenderal Kementerian Pertahanan pula, bahwa untuk sebuah sistem keamanan informasi yang menggunakan pendekatan defensif, sistem yang dimiliki Indonesia telah cukup baik.

3. Pola keterbukaan informasi pertahanan yang dimiliki Indonesia saat ini memang dinyatakan telah cukup untuk menghalau serangan terhadap informasi pertahanan yang dimiliki dalam lingkungan Kementerian Pertahanan. Meski begitu, dari penelitian ini ditemukan bahwa semua fungsi yang dimiliki oleh pemerintah Indonesia, baik melalui peran Kementerian Komunikasi dan Informatika ataupun Kementerian Pertahanan sebagai bagian penting dalam pola keterbukaan informasi pertahanan di Indonesia belum maksimal dalam melindungi keamanan informasi pertahanan di Indonesia. Di luar alasan teknis dan alasan lain yang tidak bisa dikontrol oleh kedua kementerian, sistem ini masih memiliki banyak celah yang dapat berbahaya sebagai ancaman nontradisional. Beberapa celah itu misalnya, masih lemahnya koordinasi antar kementerian yang berperan langsung dalam pola keterbukaan informasi pertahanan di Indonesia dan juga mengenai penegakan sistem keamanan informasi. Selain juga, belum maksimalnya unit kerja yang ada di dalam pola keterbukaan informasi, seperti unit Pengelolaan Opini Publik terhadap informasi bidang pertahanan. Jika unit pengelolaan opini publik ini lebih dapat menghasilkan kerja yang lebih optimal, tentu hal tersebut juga dapat berdampak pada sistem keamanan informasi pertahanan yang lebih optimal dan keamanan informasi yang lebih baik lagi.

5.2. Saran

Dalam meninjau pola keterbukaan informasi pertahanan Indonesia saat ini, diperoleh beberapa temuan yang menjadi kelebihan maupun kekurangan. Dari temuan-temuan tersebut, maka perlu adanya saran-saran agar menjadi acuan untuk peningkatan upaya mencapai keunggulan informasi, atau menjadi acuan untuk partisipasi masyarakat dalam informasi yang lebih baik lagi.

5.2.1 Saran Teoritis

Dalam hal ini perlu adanya kajian lebih lanjut mengenai teknis serta infrastruktur yang tepat dalam penggunaan melalui pola keterbukaan informasi pertahanan dan sistem keamanan informasi pertahanan. Hal tersebut bertujuan untuk melengkapi penanganan permasalahan yang cenderung bersifat teknis, baik oleh Kementerian Komunikasi dan Informatika ataupun oleh Kementerian Pertahanan. Selanjutnya diharapkan hasil penelitian ini dapat menjadi rujukan bagi penelitian-penelitian selanjutnya dengan tema atau fokus penelitian yang berbeda.

5.2.2. Saran Praktis

Keterbukaan informasi merupakan hal yang pokok dalam terwujudnya masyarakat Indonesia yang lebih demokratis. Namun, keterbukaan informasi pertahanan dapat menjadi ancaman nontradisional jika pendekatan keamanan informasi yang diterapkan kurang maksimal. Agar keterbukaan informasi pertahanan dapat lebih baik, maka perlu adanya saran-saran untuk kemajuan pola keterbukaan informasi pertahanan, yaitu sebagai berikut;

1. Sekretaris Jenderal Kementerian Pertahanan dapat meningkatkan upaya untuk mencapai kemandirian atas infrastuktur yang digunakan dalam sistem keamanan informasi pertahanan. Dimulai dari hal yang kecil seperti aplikasi dan pengembangan jaringan hingga hal yang besar seperti kepemilikan satelit pertahanan.
2. Kepala Pusat Komunikasi Publik Kementerian Pertahanan disarankan untuk melibatkan media massa dalam melakukan sosialisasi budaya keamanan nasional dan bukan menjadikan media massa sebagai lembaga yang tidak berpihak pada keterbukaan informasi pertahanan. Hal ini dapat dilakukan melalui Kepala Bidang Pemberitaan. Selain itu perlu pula untuk mengoptimalkan opini masyarakat yang didapat baik melalui media sosial atau surat menyurat sebagai produk umpan balik

terhadap perbaikan pola keterbukaan informasi pertahanan yang dimiliki Kementerian Pertahanan. Hal ini dapat dilakukan melalui Kepala Bidang Opini.

3. Kepala Bidang Pengembangan Sistem Informasi Pertahanan Kementerian Pertahanan serta Kepala Bidang Informasi dan Sandi Pusat Data dan Informasi Kementerian Pertahanan penting untuk meningkatkan suprastruktur yang terlibat dalam pola keterbukaan informasi pertahanan melalui pelatihan operasional dan manajemen teknologi kepada sumber daya manusia yang dimiliki institusi publik.
4. Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika menyediakan aplikasi atau situs yang memiliki kegunaan dan fungsi yang sama atas aplikasi atau situs yang harus ditutup karena dianggap tidak sesuai dengan UU atau tidak berpihak pada keamanan informasi pertahanan. Memperkecil jurang digital antar masyarakat Indonesia melalui pembangunan infrastruktur teknologi komunikasi dan informasi yang lebih baik di daerah-daerah terpencil.
5. Kepala Sub Direktorat Budaya Keamanan Informasi, Kementerian Komunikasi dan Informatika dapat melakukan sosialisasi budaya keamanan nasional terhadap masyarakat secara lebih menyeluruh yang melibatkan masyarakat dengan berbagai latar belakang sehingga kesadaran terhadap keamanan informasi dapat terbangun dalam berbagai lapisan masyarakat.

DAFTAR REFERENSI

REFERENSI BUKU

Afriadi dan Hersutanto B., (eds.), *Indonesia Berdaulat Bermartabat: Kompilasi Pemikiran Anggota Komisi I DPR RI 2009-2014*, RMBooks, Jakarta, 2014.

Aydinli, E., dan James N. Rosenau, *Globalization, Security, and the Nation-State: Paradigms in Transition* , New York, University of New York, 2005.

Buss, T. F., F. S. Redburn, dan K. Guo (eds), *Modernizing Democracy: Innovations in Citizen Participation,* M.E Sharpe, New York, 2006.

Clarke, R. A., dan Knake R. K., *Cyber War: The Next Threat to National Security and What to Do About It,* HarperCollins, New York, 2010.

Creswell. J. W., *Research Design Pendekatan Kualitatif, Kuantitatif, dan Mixed.* Pustaka Pelajar, Yogyakarta, 2010.

Denning, D., *Information Warfare and Security*, Addison-Weasley, Washington DC, 1999.

Evans, G. dan J. Newnham, *Dictionary of International Relations,* Penguin Books, London, 1998.

Gordon E., J. Baldwin-Philippi dan M. Balestra, *Why We Engage: How Theories of Human Behavior Contribute to Our Understanding of Civic Engagement in a Digital Era,* Berkman Center at Harvard University, Cambridge, 2013.

Grenader, U., *General Pattern Theory,*Oxford Science Publications,Oxford, 1994.

Kementerian Komunikasi dan Informatika, *Panduan Topologi dan Keamanan Sistem Informasi*, Kementerian Komunikasi dan Informatika, 2013.

Kementerian Pertahanan Republik Indonesia, *Buku Putih Pertahanan Indonesia 2008*, Kementerian Pertahanan Republik Indonesia, 2008.

Kramer, F. D., “Cyberpower and National Security: Policy Recommendations for a Strategic Framework”, dalam F. D. Kramer, S. Starr dan L. K. Wentz, eds., *Cyberpower and National Security*, Washington D.C., National Defense University Press, 2009.

Luhulima, C.P.F., ‘Kemajuan Teknologi Informasi dan Komunikasi: Saran untuk Strategi Keamanan Nasional’, dalam Bantarto Bandoro (ed.), *Perspektif Baru Keamanan Nasional*, Percetakan Kanisius, Yogyakarta, 2006.

Moleong, L. J., *Metode Penelitian Kualitatif*, PT. Remaja Rosdakarya, Bandung, 2010.

Octavian, A., *Militer dan Globalisasi*, UI Publishers, Jakarta, 2012.

Schmidt, E. dan J. Cohen, *The New Digital Age*, edisi Bahasa Indonesia, *Era Baru Digital,* diterjemahkan oleh Selviya Hanna, Kepustakaan Populer Gramedia, Jakarta, 2013.

Singer P. W., dan Friedman A., *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, New York, 2014

Stokes, J., *How to Do Media and Cultural Studies,* edisi Bahasa Indonesia, *Panduan untuk Melaksanakan Penelitian dalam Kajian Media dan Budaya,* diterjemahkan oleh Santi Indra Astuti, Bentang Pustaka, Yogyakarta, 2007.

Sun, T., *Art of War*, Shambala, Boston, 1988.

Thornton, R., *Asymmetric Warfare*, Polity Press, Cambridge, 2007.

Verba S., N. H. Nie, dan Jae-on Kim, *Participation and Political Equality: A Seven-Nation Comparison,* Cambridge University Press, Cambridge ,1978.

Yanow, D. dan P. Schwartz-Shea, eds. *Interpretation and method: Empirical research methods and the interpretive turn*, Armonk, New York, M.E. Sharpe, 2006.

Waltz, E., *Information Warfare Principles and Operations,* Artech House, London, 1998.

Wheatley, G. F., dan R. E. Hayes, *Information Warfare and Deterrence,* NDU Press Book, Washington D.C, 1996.

REFERENSI JURNAL

------, *Strategic Defence Review,* HMSO, London, 1998, bab 2

Binnendijk, H., dan R. L. Kugler, *"*Adapting Forces to a New Era: Ten Transforming Concepts", *Defense Horizon*, no.5, 2001, National Defense University, Washington DC.

Elsea, J. K., *CRS Report for Congress: Protection of National Security Information*, 2006

REFERENSI *ONLINE*

Kamus Besar Bahasa Indonesia dalam jaringan diakses dari www.kbbi.web.id

Definisi *Pattern* diakses dari www.wolframalpha.com

Tentang TRUST+ diakses dari <http://trustpositif.kominfo.go.id/>, diakses pada 2 Januari 2015.

Asrin, H., 'Sistem Informasi Pertahanan Negara Yang Terintegrasi Dalam Menghadapi Perang Informasi'*, Kementerian Pertahanan Republik Indonesia,* 21 Mei 2012,<http://www.kemhan.go.id/kemhan/?pg=73&id=204>*,* diakses pada 6 September 2014.

'DPR Diminta Serius Bahas RUU Komcad'*,Suara Pembaruan(online),* 3 September 2013, <http://sp.beritasatu.com/home/dpr-diminta-serius-bahas-ruu-komcad/41176>, diakses pada 16 Februari 2015.

'Pemerintah Harus Yakinkan Publik Soal Komcad', *Suara Pembaruan(online),* 12 Juni 2013, <http://sp.beritasatu.com/home/pemerintah-harus-yakinkan-publik-soal-komcad/36900>, diakses pada 16 Februari 2015.

'Prabowo tegaskan Tank Leopard bisa digunakan di RI, Jokowi tidak', *Merdeka.com(online),* 22 Juni 2014, <http://www.merdeka.com/politik/prabowo-tegaskan-tank-leopard-bisa-digunakan-di-ri-jokowi-tidak.html>, diakses pada 17 Februari 2015.

'Terancam Kehilangan Kewenangan, Polri Pasrah', *Hukum Online*, 1 Februari 2012, <http://www.hukumonline.com/berita/baca/lt4f294054bf522/terancam-kehilangan-kewenangan-polri-pasrah>, diakses pada 17 Februari 2015.

Pusat Kodifikasi Kementerian Pertahanan, 2011, <http://ncb45.or.id/index.php?mod=content&cmd=loadcontent&id=19>*,* diakses pada 28 Desember 2014.

Pusat Data dan Informasi Kementerian Pertahanan, *Struktur Organisasi Pusdatin Kemhan (online),* <http://pusdatin.kemhan.go.id/?pg=142>*,* diakses pada 28 Desember 2014.

Pejabat Pengelola Informasi dan Dokumentasi, *Struktur Organisasi (online),* <http://ppid.kominfo.go.id/about/kemkominfo/struktur/>*,* diakses pada 27 Desember 2014.

Pusat Monitoring dan Penanganan Insiden Keamanan Informasi Kementerian Komunikasi dan Informatika, *Statistik Insiden Respon Domain .go.id (online),* <http://govcsirt.kominfo.go.id/insiden-defacement-terjadi-di-situs-pemerintahan/>*,* diakses pada 1 Januari 2015.

REFERENSI UNDANG-UNDANG

Sekretariat Komisi Informasi Pusat, *Undang-Undang Republik Indonesia Nomor 14 Tahun 2008,* 2010.

Kementerian Komunikasi dan Informatika Republik Indonesia, *Undang-Undang Republik Indonesia No.14 Tahun 2008 tentang Keterbukaan Informasi Publik*, Kementerian Komunikasi dan Informatika Republik Indonesia, 2013.

Joint Chiefs of Staff, *Joint Vision 2010*, U.S. Department of Defense, Washington D.C., July 1997.

Edaran Peraturan Menteri Pertahanan Nomor 16 Tahun 2010.

Keputusan Menteri Pertahanan KEP/1040/M/ XII/2011 tentang Informasi Pertahanan yang Dikecualikan di Lingkungan Kementerian Pertahanan.

Keputusan Menteri Pertahanan KEP/538/M/VII/2012 tentang Informasi Pertahanan di Lingkungan Kementerian Pertahanan.

DAFTAR LAMPIRAN

Lampiran 1. Daftar Narasumber

1. Sekretaris Jenderal Kementerian Pertahanan
2. Kepala Sub Bidang Informasi, Bidang Kerjasama Informasi Pusat Komunikasi Publik Kementerian Pertahanan
3. *Defense Media Center* Kementerian Pertahanan
4. Kepala Data dan Informasi Strategi Pertahanan Kementerian Pertahanan
5. Kepala Bidang Pengembangan Sistem Informasi Pertahanan Kementerian Pertahanan
6. Kepala Bidang Informasi dan Sandi Pusat Data dan Informasi Kementerian Pertahanan
7. Kepala Sub Bidang Pembinaan Fungsi Dinas Informasi dan Pengolahan Data TNI Angkatan Darat
8. Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika
9. Kepala Sub Direktorat Budaya Keamanan Informasi, Kementerian Komunikasi dan Informatika

Lampiran 2. Petunjuk Umum Wawancara

Petunjuk umum wawancara ini untuk beberapa narasumber, yaitu Sekretaris Jenderal Kementerian Pertahanan, Kepala Sub Bidang Informasi, Bidang Kerjasama Informasi Pusat Komunikasi Publik Kementerian Pertahanan, Kepala Data dan Informasi Strategi Pertahanan Kementerian Pertahanan, Kepala Bidang Pengembangan Sistem Informasi Pertahanan Kementerian Pertahanan, Kepala Sub Bidang Pembinaan Fungsi Dinas Informasi dan Pengolahan Data TNI Angkatan Darat.

Informasi Umum

NARASUMBER 1

Nama : Letnan Jenderal Ediwan Prabowo
Jenis kelamin : Laki-laki
Jabatan : Sekretaris Jenderal (Sekjen)
Dinas/Instansi : Kementerian Pertahanan
Tempat wawancara : Kantor Sekjen Kementerian Pertahanan
Waktu wawancara : 24 November 2014 pukul 15.30 WIB

NARASUMBER 2

Nama : Letnan Kolonel Trisatya Wicaksono
Jenis kelamin : Laki-laki
Jabatan : Kepala Sub Bidang Informasi
Dinas/Instansi : Pusat Komunikasi Publik, Kementerian Pertahanan
Tempat wawancara : Kantor Pusat Komunikasi Publik
Waktu wawancara : 5 Februari 2015 pukul 09.30 WIB

NARASUMBER 3

Nama	: Kolonel Dominggus Pakel
Jenis kelamin	: Laki-laki
Jabatan	: Kepala Bidang Informasi dan Persandian merangkap Kepala Bidang Pengembangan Sistem Informasi Pertahanan
Dinas/Instansi	: Pusat Data dan Informasi, Kementerian Pertahanan
Tempat wawancara	: Kantor Pusat Data dan Informasi
Waktu wawancara	: 1 Desember 2014 pukul 09.30 WIB

NARASUMBER 4

Nama	: Kolonel Ir. Ignatius Budiman S. Pratomo
Jenis kelamin	: Laki-laki
Jabatan	: Kepala Sub Bidang Pembinaan Fungsi
Dinas/Instansi	: Dinas Informasi dan Pengolahan Data TNI-AD
Tempat wawancara	: Kantor Dinas Informasi dan Pengolahan Data, Markas Besar Angkatan Darat
Waktu wawancara	: 23 Januari 2015 pukul 09.30 WIB

Pertanyaan Penelitian

Ajuan Pertanyaan Wawancara

Fauzia Gustarina Cempaka Timur
Mahasiswa Universitas Pertahanan Indonesia
Judul Tesis: Pola Keterbukaan Informasi Bidang Pertahanan di Indonesia sebagai Ancaman Nontradisional

1. Bagaimana institusi Bapak memetakan ancaman terhadap keamanan dan pertahanan Indonesia saat ini?
2. Apakah menurut institusi Bapak, peperangan informasi merupakan ancaman nontradisional bagi Indonesia saat ini. Jika ya, kerugian apa yang dapat dan telah timbul? Jika tidak, mengapa?
3. Apakah institusi Bapak memberikan perhatian khusus terhadap peperangan informasi dan peperangan siber? Jika ya, bagaimana bentuknya? Jika tidak, mengapa?
4. Apakah UU nomor 14 tahun 2008 mengenai keterbukaan informasi publik memiliki dampak terhadap persebaran informasi di institusi Bapak?
5. Kebijakan apa sajakah yang telah diterapkan di institusi Bapak untuk mengantisipasi akibat yang dapat timbul dari peperangan informasi?
6. Bagaimana kesiapan institusi bapak baik aspek infrastruktur maupun aspek sumber daya manusia dalam melakukan antisipasi peperangan informasi?Apa kekurangan masing-masing aspek?
7. Apa saja tugas pokok dan fungsi dari instititusi Bapak yang terkait dengan pengamanan informasi?
8. Apakah kebijakan yang Bapak terapkan dianggap cukup untuk mengantisipasi peperangan informasi meskipun orang bisa melakukan *hack* atau memanfaatkan cara lain untuk mendapatkan informasi yang diinginkannya?
9. Bagaimana koordinasi yang dilakukan oleh institusi Bapak dengan institusi lain untuk melakukan antisipasi tersebut?
10. Menurut Bapak, hal-hal apa sajakah yang masih menjadi kekurangan dan dan harus ditingkatkan dalam keterbukaan Informasi?
11. Menurut Bapak, bagaimana pola keterbukaan informasi yang tepat untuk Indonesia sebagai negara demokrasi, terutama informasi yang berkaitan dengan pertahanan dan keamanan Indonesia?
12. Apa saran yang dapat Bapak berikan untuk dapat mengantisipasi dampak buruk dari keterbukaan informasi Indonesia miliki?

Lampiran 3. Surat Izin Penelitian

KEMENTERIAN PERTAHANAN RI
UNIVERSITAS PERTAHANAN

Nomor : B / 2208 / X /2014
Klasifikasi : Biasa
Lampiran : -
Hal : Permohonan izin penelitian

Jakarta, 6 Oktober 2014

Kepada
Yth.

di
Jakarta

1. Dasar :
   a. Peraturan Presiden RI Nomor : 5 Tahun 2011 tanggal 7 Februari 2011 tentang Universitas Pertahanan sebagai Perguruan Tinggi yang diselenggarakan oleh Pemerintah.
   b. Kalender Pendidikan Program Studi Peperangan Asimetris Fakultas Strategi Pertahanan Unhan TA 2013/2014.
2. Sehubungan dasar tersebut di atas, mohon dapatnya Kepala berkenan mengizinkan mahasiswa Prodi Studi Peperangan Asimetris Fakultas Strategi Pertahanan Unhan atas nama Fauziah Gustarina Cempaka Timur Nomor Mahasiswa 120130102008, untuk melaksanakan wawancara dan atau memberikan kuesioner guna mengumpulkan data-data penelitian yang diperlukan dalam penyusunan Tesis dengan judul "Pola Keterbukaan Informasi Bidang Pertahanan di Indonesia sebagai Ancaman Nontradisional".
3. Mohon konfirmasi waktu serta tempat pelaksanaan wawancara dan pemberian kuesioner. *Contact Person* : E-mail fgcempaka@gmail.com.
4. Demikian untuk menjadikan periksa.

a.n. Rektor
Universitas Pertahanan
Warek II Bid. Umum & Keuangan,

I Wayan Midhio, M.Phil
Mayor Jenderal TNI

Tembusan :
1. Rektor Unhan
2. Warek I Unhan
3. Karo Akademik & Kemahasiswaan Unhan

Komplek IPSC Sentul Bogor

Lampiran 4. Daftar Informasi Pertahanan di Lingkungan Kementerian Pertahanan

Lampiran Keputusan Menteri Pertahanan
Nomor : KEP/538/M/VII/2012
Tanggal : 2 Juli 2012

DAFTAR INFORMASI PERTAHANAN
DI LINGKUNGAN KEMENTERIAN PERTAHANAN

NO		SATKER	PERIHAL	PENANGGUNG JAWAB PEMBUATAN	WAKTU DAN TEMPAT PEMBUATAN	FORMAT INFORMASI	JANGKA WAKTU PENYIMPANAN	KETERANGAN
1	2	3	4	5	6	7	8	9
1.		**SETJEN**						
	a.	**Biro Perencanaan**	**1. Informasi yang Wajib Disediakan dan Diumumkan Secara Berkala**	Nihil	Nihil	Nihil	Nihil	Nihil
			2. Informasi yang Wajib Tersedia Setiap Saat					
			a. Penugasan dan Perijinan Keluar Negeri di Lingkungan Departemen Pertahanan	Karoren	2009	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 14 Tahun 2009 Tanggal 9 Juli 2009
			b. Organisasi dan Tata Kerja Kementerian Pertahanan	Karoren	2010	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 16 Tahun 2010 Tanggal 27 September 2010
			c. Susunan dan Tata Kerja Jabatan Fungsional Tertentu dan Fungsional Umum Kementerian Pertahanan	Karoren	2011	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 01 Tahun 2011 Tanggal 20 Januari 2011
			d. Hari dan Jam Kerja di Kementerian Pertahanan dan Tentara Nasional Indonesia	Karoren	2011	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 22 Tahun 2011 Tanggal 18 Oktober 2011
			e. Pedoman Penyusunan Analisa Beban Kerja di Lingkungan Kementerian Pertahanan	Karoren	2011	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 23 Tahun 2011 Tanggal 18 Oktober 2011
			f. Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintahan di Lingkungan Kementerian Pertahanan	Karoren	2011	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 27 Tahun 2011 Tanggal 9 November 2011
			g. Pedoman Penetapan Indikator Kinerja Utama di lingkungan Kementerian Pertahanan	Karoren	2011	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 29 Tahun 2011 Tanggal 24 November 2011
			h. Standarisasi Sarana dan Prasarana Kerja Pejabat Kementerian Pertahanan	Karoren	2011	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 35 Tahun 2011 Tanggal 30 Desember 2011
			i. Pemberian dan Pemotongan Tunjangan Kinerja kepada Pegawai di Lingkungan Kementerian Pertahanan	Karoren	2012	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 09 Tahun 2012 Tanggal 29 Februari 2012
			j. Kedudukan dan Tugas Wakil Menteri Pertahanan	Karoren	2012	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 12 Tahun 2012 Tanggal 30 Maret 2012
			k. Pakaian Seragam PNS di Lingkungan Kementerian Pertahanan	Karoren	2009	Hardcopy/ Softcopy	5 Tahun	Kepmenhan Nomor KEP/ 68/M/V/2009 Tanggal 5 Mei 2009
			l. Standar Tatalaksana Eselon II Kementerian Pertahanan	Karoren	2011	Hardcopy/ Softcopy	5 Tahun	Kepmenhan Nomor KEP/ 737/M/IX/2011 Tanggal 30 September 2011
			m. Roadmap Reformasi Birokrasi Tahun 2010-2014 Kementerian Pertahanan	Karoren	2011	Hardcopy/ Softcopy	5 Tahun	Kepmenhan Nomor KEP/ 101/ M/XII/2011 Tanggal 27 Desember 2011
			n. Standar Kompetensi Jabatan Struktural di Lingkungan Kementerian Pertahanan	Karoren	2011	Hardcopy/ Softcopy	5 Tahun	Kepmenhan Nomor KEP/ 463/ M/VI/2011 Tanggal 23 Juni 2011

1	2	3	4	5	6	7	8	9
			o. Standar Operasional Prosedur Administrasi Pemerintahan di Lingkungan Kementerian Pertahanan	Karoren	2011	Hardcopy/ Softcopy	5 Tahun	Kepmenhan Nomor KEP/ 997/ M/XII/2011 Tanggal 23 Desember 2011
			p. Indikator Dan Target Kinerja Serta Uraian Tugas di Lingkungan Kemhan	Karoren	2011	Hardcopy/ Softcopy	5 Tahun	Kepmenhan Nomor KEP/ 231/ M/IV/2011 Tanggal 2 April 2011
			q. Uraian Jabatan Struktural Eselon II, III dan IV di Lingkungan Kemhan	Karoren	2011	Hardcopy/ Softcopy	5 Tahun	Kepmenhan Nomor KEP/ 918/ M/XI/2011 Tanggal 30 November 2011
			r. Penetapan Hasil Pengukuran Beban Kerja Satuan Kerja/Sub Satuan Kerja di Lingkungan Kementerian Pertahanan	Karoren	2011	Hardcopy/ Softcopy	5 Tahun	Kepmenhan Nomor KEP/135/ M/II/2012 Tanggal 27 Februari 2012
			s. Prosedur Pemeliharaan di Lingkungan U.O. Departemen Pertahanan	Karoren	2009	Hardcopy/ Softcopy	5 Tahun	Petunjuk Pelaksanaan Nomor Juklak/01/VII/2009 Tanggal 15 Juli 2009
			t. Pedoman Penyusunan Laporan Akuntabilitas Kinerja Satuan Kerja/Sub Satuan Kerja di Lingkungan UO Kementerian Pertahanan	Karoren	2011	Hardcopy/ Softcopy	5 Tahun	Petunjuk Teknis Nomor Juknis/01/XI/2011 Tanggal 8 November 2011
			3. Informasi yang Wajib Diumumkan Secara Serta Merta	Nihil	Nihil	Nihil	Nihil	Nihil
			4. Informasi Terbuka Lainnya yang Diminta Pemohon Informasi Pertahanan	Nihil	Nihil	Nihil	Nihil	Nihil
	b.	**Biro Kepegawaian**	**1. Informasi yang Wajib Disediakan dan Diumumkan Secara Berkala**					
			a. Kenaikan Pangkat	Karopeg	2006	Hardcopy/ Softcopy	1 Tahun	Permenhan Nomor 6 Tahun 2010 Tanggal 21 Mei 2010

1	2	3	4	5	6	7	8	9
			b. Jabatan Struktural dan Fungsional	Karopeg	2010	Hardcopy/ Softcopy	1 Tahun	Permenhan Nomor PER/02/ M/V/2006
			c. Tanda Jasa	Karopeg	1992	Hardcopy/ Softcopy	5 Tahun	Kepmenhan/ Pangab Nomor 04/VI/92 Tanggal 9 Juni 1992 tentang Administrasi Penganu-gerahan Tanda Jasa Jenis Bintang
			d. Pemisahan PNS	Karopeg	2008	Hardcopy/ Softcopy	10 Tahun	Permenhan Nomor 22 Tahun 2010
			e. Pelatihan Ketrampilan	Karopeg	2007	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor PER/11/ M/XII/2007
			2. Informasi yang Wajib Tersedia Setiap Saat					
			a. Peraturan Penilaian Kompetensi Individu Pegawai Di Lingkungan Kementerian Pertahanan	Karopeg	2011	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 4 Tahun 2011 Tanggal 28 Maret 2011
			b. Peraturan Penyelenggaraan Ujian Dinas PNS Kementerian Pertahanan	Karopeg	2009	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 8 Tahun 2009
			c. Penyelenggaraan Ujian Penyesuaian Kenaikan Pangkat PNS Kementerian Pertahanan	Karopeg	2010	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 6 Tahun 2010 Tanggal 21 Mei 2010
			d. Pedoman Peribadatan Bagi Pegawai di Lingkungan Kementerian Pertahanan	Karopeg	2008	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 22 Tahun 2008
			e. Peraturan Perkawinan, Perceraian dan Rujuk Bagi Pegawai di Lingkungan Kementerian Pertahanan	Karopeg	2008	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 23 Tahun 2008

1	2	3	4	5	6	7	8	9
			f. Pembekalan Pelatihan Keterampilan Kerja Pegawai Kementerian Pertahanan	Karopeg	2008	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor PER/11/ M/XII/2007
			g. Tatacara Penjatuhan Hukuman Disiplin Bagi PNS Kementerian Pertahanan	Karopeg	2008	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 22 Tahun 2010
			h. Ketentuan Jabatan Fungsional PNS Kementerian Pertahanan	Karopeg	2008	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor PER/02/ M/V/2006
			i. Pelaksanaan Jabfung Analis Kepegawaian dan Angka Kreditnya Bagi PNS Kementerian Pertahanan	Karopeg	2008	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 28 Tahun 2009
			j. Penyelenggaraan Pengadaan CPNS Kementerian Pertahanan	Karopeg	2010	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 08 Tahun 2008
			k. Pokok – Pokok Pembinaan PNS Kementerian Pertahanan	Karopeg	2009	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 09 Tahun 2009
			l. Pedoman Diklat Pegawai Kementerian Pertahanan	Karopeg	2009	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 14 Tahun 2009
			m. Pelaksanaan Jabfung Auditor dan Angka Kreditnya bagi PNS Kementerian Pertahanan	Karopeg	2008	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 07 Tahun 2009
			n. Pelaksanaan Jabfung Pranata Komputer dan Angka Kreditnya Bagi PNS Kementerian Pertahanan	Karopeg	2009	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 04 Tahun 2009
			o. Pelaksanaan Jabfung Widyaiswara dan Angka Kreditnya Bagi PNS Kementerian Pertahanan	Karopeg	2009	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 01 Tahun 2009

1	2	3	4	5	6	7	8	9
			3. Informasi Yang Wajib Diumumkan Secara Serta Merta					
			a. Pengadaan CPNS	Karopeg	2008	Hardcopy/ Softcopy	1 Tahun	Permenhan Nomor 08 Tahun 2008
			b. Dik Bang Um & Dik Bang Spes	Karopeg	2008	Hardcopy/ Softcopy	1 Tahun	Permenhan Nomor 14 Tahun 2008
			4. Informasi Terbuka Lainnya yang Diminta Pemohon Informasi Pertahanan	Nihil	Nihil	Nihil	Nihil	Nihil
	c.	**Biro Hukum**	**1. Informasi yang Wajib Disediakan dan Diumumkan Secara Berkala**	Nihil	Nihil	Nihil	Nihil	Nihil
			2. Informasi yang Wajib Tersedia Setiap Saat					
			a. Bantuan Hukum di Lingkungan Kemhan	Karokum	2012	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 22 Tahun 2012
			b. Teknik Penyusunan Permen - han	Karokum	2008	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 35 Tahun 2008 Tanggal 31 Desember 2008
			3. Informasi Yang Wajib Tersedia Secara Serta Merta					
			- Keputusan Pengadilan	Majelis Hakim Pengadilan	2006 s.d 2012	Hardcopy	Sesuai ketentuan yang berlaku	UU Nomor 48 Tahun 2009 Tanggal 29 Oktober 2009 tentang Kekuasaan Kehakiman
			4. Informasi Terbuka Lainnya yang Diminta Pemohon Informasi Pertahanan	Nihil	Nihil	Nihil	Nihil	Nihil

1	2	3	4	5	6	7	8	9
	d.	**Biro Tata Usaha**	**1. Informasi yang Wajib Disediakan dan Diumumkan Secara Berkala**					
			a. Kegiatan Menteri	Karo TU	2012	Hardcopy/ Softcopy	1 Tahun	-
			b. Kegiatan Wamen	Karo TU	2012	Hardcopy/ Softcopy	1 Tahun	-
			c. Kegiatan Sekjen	Karo TU	2012	Hardcopy/ Softcopy	1 Tahun	-
			2. Informasi yang Wajib Tersedia Setiap Saat					
			a. Petunjuk Pelaksanaan Jabatan Fungsional Arsiparis dan Angka Kreditnya serta Tunjangan Jabatannya di Lingkungan Kemhan	Karo TU	2004	Hardcopy/ Softcopy	Sampai ada perubahan	Juklak Nomor SKEP/338/ IV/2004 Tanggal 28 April 2004
			b. Petunjuk Pelaksanaan Penilaian Prestasi Kerja Arsiparis Departemen Pertahanan	Karo TU	2004	Hardcopy/ Softcopy	Sampai ada perubahan	Juklak Nomor SKEP/339/ IV/2004 Tanggal 30 April 2004
			c. Peraturan Peningkatan Pengamanan Pengelolaan Surat/ Tulisan Dinas di Lingkungan Departemen Pertahanan	Karo TU	2006	Hardcopy/ Softcopy	Sampai ada perubahan	Permenhan Nomor PER/ 15/M/IX/2006 Tanggal 30 November 2006
			d. Pedoman Penyusunan Formasi Jabatan Fungsional Arsiparis Kementerian Pertahanan	Karo TU	2010	Hardcopy/ Softcopy	Sampai ada perubahan	Permenhan Nomor 29 Tahun 2010 Tanggal 31 Desember 2010
			e. Pedoman Kearsipan di Lingkungan Kemhan dan TNI	Karo TU	2010	Hardcopy/ Softcopy	Sampai ada perubahan	Permenhan Nomor 30 Tahun 2010 Tanggal 31 Desember 2010

1	2	3	4	5	6	7	8	9
			f. Pedoman Pengelolaan Arsip Dinamis Kemhan dan TNI	Karo TU	2011	Hardcopy/ Softcopy	Sampai ada perubahan	Permenhan Nomor 18 Tahun 2011 Tanggal 13 September 2011
			g. Pedoman Administrasi Umum Kemhan	Karo TU	2012	Hardcopy/ Softcopy	Sampai ada perubahan	Permenhan Nomor 04 Tahun 2012 Tanggal 8 Februari 2012
			h. Pedoman Penyusutan Arsip Kemhan dan TNI	Karo TU	2012	Hardcopy/ Softcopy	Sampai ada perubahan	Permenhan Nomor 05 Tahun 2012 Tanggal 8 Februari 2012
			3. Informasi yang Wajib Diumumkan Secara Serta Merta	Nihil	Nihil	Nihil	Nihil	Nihil
			4. Informasi Terbuka Lainnya yang Diminta Pemohon Informasi Pertahanan	Nihil	Nihil	Nihil	Nihil	Nihil
	e.	**Biro Umum**	**1. Informasi yang Wajib Disediakan dan Diumumkan Secara Berkala**					
			- Pengadaan Barang dan Jasa terpusat UO Kemhan yang dilaksanakan di Biro Umum	Karoum	Tahunan	Hardcopy/ Softcopy	1 Tahun	Website Kemhan
			2. Informasi yang Wajib Tersedia Setiap Saat					
			a. Peraturan Urusan Dinas Dalam khusus Kemhan	Karoum	2008	Hardcopy	1 Tahun	Permenhan Nomor 41 Tahun 2008 tanggal 30 Desember 2008
			b. Tata Upacara di lingkungan Kemhan	Karoum	2008	Hardcopy	1 Tahun	Skep Panglima TNI Nomor Skep/292 Tanggal 6 September 2004

1	2	3	4	5	6	7	8	9
			c. Protap tentang Pencegahan dan Penanggulangan bahaya kebakaran di lingkungan Dephan	Karoum	2007	Hardcopy	1 Tahun	Protap Nomor 03/VI/2007 Tanggal 22 Juni 2007
			d. Pengamanan kelling komplek Kemhan terhadap ancaman/serangan dari Luar/Dalam (*Alarm of Stelling*) tahun 2006	Karoum	2006	Hardcopy	1 Tahun	Protap Nomor 03/VI/2007 Tanggal 22 Juni 2007
			e. Tata cara Upacara pengangkatan sumpah dan pelantikan serta serah terima jabatan di lingkungan UO Kemhan	Karoum	2003	Hardcopy	10 Tahun	Petunjuk Teknis Nomor Juknis/01/XII/2003 Tanggal 17 Desember 2003
			f. Penomoran Registrasi dan Penggunaan Logo Kemhan pada Kendaraan Bermotor di Lingkungan Kemhan	Karoum	2012	Hardcopy	1 Tahun	Petunjuk Pelaksanaan Nomor Juklak/06/III/2012 Tanggal 15 Maret 2012
			g. Tata Cara Pelaporan Korps Raport kenaikan pangkat bagi personil TNI dan PNS di Lingkungan Unit Organisasi Kemhan	Karoum	2006	Hardcopy	10 Tahun	Petunjuk Teknis Nomor Juknis /01/XII/2003 Tanggal 17 Desember 2003
			3. Informasi Yang Wajib Diumumkan Secara Serta Merta					
			- Penghematan Energi Listrik, Telepon & Air di Lingkungan Kemhan	Karoum	2011	Hardcopy/ Softcopy	1 Tahun	SE Nomor SE/30/2011 Tanggal 15 September 2011

1	2	3	4	5	6	7	8	9
			4. Informasi Terbuka Lainnya yang Diminta Pemohon Informasi Pertahanan	Nihil	Nihil	Nihil	Nihil	Nihil
2.		ITJEN	**1. Informasi yang Wajib Disediakan dan Diumumkan Secara Berkala**					
			- Jadwal Pemeriksaan	Irjen Kemhan	2011	Hardcopy/ Softcopy	1 Tahun	Website Kemhan
			2. Informasi yang Wajib Tersedia Setiap Saat					
			a. Petunjuk Teknis Pengoperasian Aplikasi Pengawasan dan Pemeriksaan	Irjen Kemhan	2007	Hardcopy/ Softcopy	Sampai ada pemeriksaan	Skep/037/XII/2007 Tanggal 28 Desember 2007
			b. Kunjungan Kerja	Irjen Kemhan	2009	Hardcopy/ Softcopy	Sampai ada pemeriksaan	Petunjuk Teknis Nomor Juknis/002/IX/2009 Tanggal 15 September 2009
			c. Pengawasan dan Intern di Lingkungan Kemhan	Irjen Kemhan	2010	Hardcopy/ Softcopy	Sampai ada pemeriksaan	Petunjuk Pelaksanaan Nomor Juklak/03/XII/2010 Tanggal 31 Desember 2012
			d. Pemeriksaan dengan tujuan tertentu (PDTT) di lingkungan Kemhan	Irjen Kemhan	2011	Hardcopy/ Softcopy	Sampai ada pemeriksaan	Petunjuk Teknis Nomor Juknis/001/VIII/2011 Tanggal 8 Agustus 2011
			e. Pengawasan dan Pemeriksaan Bidang Logistik Pengelolaan BMN di Lingkungan Kemhan dan TNI	Irjen Kemhan	2011	Hardcopy/ Softcopy	Sampai ada pemeriksaan	Petunjuk Teknis Nomor Juknis/03/VII/2011 Tanggal 19 Juli 2011

1	2	3	4	5	6	7	8	9
			f. Evaluasi Akuntabilitas Kinerja Instansi Pemerintah di Lingkungan Unit Organisasi Kemhan	Irjen Kemhan	2011	Hardcopy/ Softcopy	Sampai ada pemeriksaan	Petunjuk Pelaksanaan Nomor Juklak/02/XII/2011 Tanggal 2 Desember 2011
			g. Pedoman Pengawasan dan Pemeriksaan terhadap Pelaksanaan Tugas Pertahanan	Irjen Kemhan	2011	Hardcopy/ Softcopy	Sampai ada pemeriksaan	Petunjuk Teknis Nomor Juknis/03/XII/2011 Tanggal 15 Desember 2011
			h. Pengawasan dan Pemeriksaan Bidang Umum Sumber Daya Manusia	Irjen Kemhan	2011	Hardcopy/ Softcopy	Sampai ada pemeriksaan	Petunjuk Teknis Nomor Juknis/05/XII/2011 Tanggal 26 Desember 2011
			i. Pengawasan dan Pemeriksaan Bidang Pengadaan Barang di Lingkungan Kemhan dan TNI	Irjen Kemhan	2011	Hardcopy/ Softcopy	Sampai ada pemeriksaan	Petunjuk Teknis Nomor Juknis/06/XII/2011 Tanggal 26 Desember 2011
			j. Reviu Laporan Keuangan Kemhan dan TNI	Irjen Kemhan	2011	Hardcopy/ Softcopy	Sampai ada pemeriksaan	Petunjuk Pelaksanaan Nomor Juklak/04/XII/2011 Tanggal 30 Desember 2011
			3. Informasi Yang Wajib Diumumkan Secara Serta Merta					
			- Program Kerja Pemeriksaan Tahunan (PKPT)	Irjen Kemhan	2012	Hardcopy/ Softcopy	1 Tahun	Website Itjen Kemhan
			4. Informasi Terbuka Lainnya yang diminta Pemohon Informasi Pertahanan	Nihil	Nihil	Nihil	Nihil	Nihil
3.		**DITJEN STRAHAN**	**1. Informasi yang Wajib Disediakan dan Diumumkan Secara Berkala**					
			a. Leaflet Ditjen Strahan TA. 2012	Dirjen Strahan	Tahunan	Hardcopy/ Softcopy	5 Tahun	Perpustakaan

1	2	3	4	5	6	7	8	9
			b. Booklet Profil Ditjen Strahan TA. 2012	Dirjen Strahan	Tahunan	Hardcopy/ Softcopy	5 Tahun	Perpustakaan
			c. Profil Ditjen Strahan TA. 2012	Dirjen Strahan	Tahunan	Hardcopy/ Softcopy	5 Tahun	Perpustakaan
			d. Majalah Ditjen Strahan TA. 2012	Dirjen Strahan	Tahunan	Hardcopy/ Softcopy	5 Tahun	Perpustakaan
			2. Informasi yang Wajib Tersedia Setiap Saat					
			a. Produk kebijakan Pertahanan Negara yang dibuat oleh Kementerian Pertahanan	Dirjen Strahan	2010	Hardcopy/ Softcopy	5 Tahun	Permenhan dan Kepmen
			b. Buku Putih Pertahanan Negara	Dirjen Strahan	2008	Hardcopy/ Softcopy	5 Tahun	Website Ditjen Strahan
			c. Produk kajian yang tidak bersifat rahasia yang dibuat di lingkungan Ditjen Strahan	Dirjen Strahan	Tahunan	Hardcopy/ Softcopy	5 Tahun	Website Ditjen Strahan
			d. Kegiatan yang tidak bersifat rahasia dan kegiatan lain yang boleh dipublikasikan dan yang dibuat di lingkungan Ditjen Strahan	Dirjen Strahan	Harian	Hardcopy/ Softcopy	1 Tahun	Website Ditjen Strahan
			e. Peraturan perundang-undangan yang terkait dengan Pertahanan Negara	Dirjen Strahan	Tahunan	Hardcopy/ Softcopy	5 Tahun	Website Ditjen Strahan
			3. Informasi Yang Wajib Diumumkan Secara Serta Merta					
			- Situasi Dalam Negeri dan Luar Negeri yang berpotensi mengancam keselamatan umum dan mengancam jiwa orang lain	Ditjen Strahan	Tahunan	Hardcopy/ Softcopy	1 Tahun	Website Ditjen Strahan

1	2	3	4	5	6	7	8	9
			4. Informasi Terbuka Lainnya yang Diminta Pemohon Informasi Pertahanan	Nihil	Nihil	Nihil	Nihil	Nihil
4.		**DITJEN RENHAN**	**1. Informasi yang Wajib Disediakan dan Diumumkan Secara Berkala**					
			- Rekapitulasi Laporan Realisasi Anggaran Audited	Dirjen Renhan	Tahunan	Hardcopy/ Softcopy	10 Tahun	UU Nomor 14 Tahun 2008, PP Nomor 61 Tahun 2010, Permenhan Nomor 14 Tahun 2011
			2. Informasi yang Wajib Tersedia Setiap Saat					
			a. Pedoman Pelaksanaan Pelaporan Keuangan dan Kinerja di Lingkungan Kemhan dan TNI	Dirjen Renhan	2010	Hardcopy/ Softcopy	5 Tahun	Per Dirjen Renhan Nomor 04 Tahun 2010
			b. Perawatan dan Pemakaman Jenazah Prajurit TNI/Purnawira wan dan PNS/Wredatama di lingkungan Kemhan dan TNI	Dirjen Renhan	2010	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 25 Tahun 2010
			c. Tunjangan Operasi Pengaman an bagi Prajurit TNI dan PNS yang bertugas operasi pengaman pada pulau-pulau kecil terluar dan wilayah perbatasan	Dirjen Renhan	2010	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 10 Tahun 2010
			d. Pedoman Pelaksanaan Tunjangan Operasi Pengaman an bagi Prajurit TNI dan PNS yang bertugas dalam operasi pengaman pada pulau-pulau kecil terluar dan wilayah perbatasan	Dirjen Renhan	2010	Hardcopy/ Softcopy	5 Tahun	Per Dirjen Renhan Kemhan Nomor 12 Tahun 2010

1	2	3	4	5	6	7	8	9
			e. Pedoman Pelaksanaan Penge-lolaan Iuran Dana Pensiun di lingkungan Kemhan dan TNI pada PT. ASABRI (PERSERO)	Dirjen Renhan	2010	Hardcopy/ Softcopy	5 Tahun	Perdirjen Renhan Kemhan Nomor 01 Tahun 2010
			f. Tunjangan Kinerja di lingkungan Kemhan dan TNI	Dirjen Renhan	2011	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 32 Tahun 2011
			g. Pedoman Pembentukan dan Pembiayaan Pokja di lingkungan Kemhan dan TNI	Dirjen Renhan	2011	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 33 Tahun 2011
			h. Pengelolaan Keuangan BLU di lingkungan Kemhan dan TNI	Dirjen Renhan	2011	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 28 Tahun 2011
			i. Biaya Perjalanan Dinas Jabatan Dalam Negeri, Pegawai Negeri dan Pegawai Tidak Tetap di Lingkungan Kemhan dan TNI	Dirjen Renhan	2011	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 37 Tahun 2011
			j. Dokumen Perkembangan Anggaran	Dirjen Renhan	2011	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 37 Tahun 2011
			k. SPP Hanneg	Dirjen Renhan	2009	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 10 Tahun 2009
			l. Penelitian dan Pengembangan bidang Pertahanan di lingkungan Kemhan dan TNI	Dirjen Renhan	2011	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 39 Tahun 2011 Tanggal 30 Desember 2011
			m. Sistem Akuntabilitas Kinerja Instansi Pemerintah	Dirjen Renhan	2011	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 39 Tahun 2011 Tanggal 30 Desember 2011
			3. Informasi Yang Wajib Diumumkan Secara Serta Merta	Nihil	Nihil	Nihil	Nihil	Nihil
			4. Informasi Terbuka Lainnya yang Diminta Pemohon Informasi Pertahanan	Nihil	Nihil	Nihil	Nihil	Nihil

1	2	3	4	5	6	7	8	9
5.		DITJEN POTHAN	**1. Informasi yang Wajib Disediakan dan Diumumkan Secara Berkala**					
			a. Booklet Ditjen Pothan	Dirjen Pothan	Tahunan	Hardcopy/ Softcopy	1 Tahun	Website Ditjen Pothan
			b. Leaflet PKBN	Dirjen Pothan	Tahunan	Hardcopy/ Softcopy	1 Tahun	Website Ditjen Pothan
			c. Majalah Veteran	Dirjen Pothan	Tahunan	Hardcopy/ Softcopy	1 Tahun	Website Ditjen Pothan
			2. Informasi yang Wajib Tersedia Setiap Saat					
			a. Rancangan Undang-Undang Komponen Cadangan	Dirjen Pothan	2009	Hardcopy/ Softcopy	Selama belum ada perubahan	Dalam Proses Pembahasan
			b. Rancangan Undang-Undang Kamnas	Dirjen Pothan	2010	Hardcopy/ Softcopy	Selama belum ada perubahan	Dalam Proses Pembahasan
			c. Visi dan Misi Ditjen Pothan Kemhan	Dirjen Pothan	2011	Hardcopy/ Softcopy	5 Tahun	Website Ditjen Pothan
			d. Kebijakan Ditjen Pothan	Dirjen Pothan	2011	-	1 Tahun	Website Ditjen Pothan
			e. Kegiatan Ditjen Pothan	Dirjen Pothan	2011	-	1 Tahun	Website Ditjen Pothan
			3. Informasi yang Wajib Diumumkan Secara Serta Merta					
			a. Uji Fungsi Surveyliance System	Dirjen Pothan	2008	Hardcopy	2 Tahun	Website Pothan
			b. Uji Coba Roket R-Han122	Dirjen Pothan	2011	Hardcopy	5 Tahun	Website Pothan
			4. Informasi Terbuka Lainnya yang Diminta Pemohon Informasi Pertahanan	Nihil	Nihil	Nihil	Nihil	Nihil

1	2	3	4	5	6	7	8	9
6.		DITJEN KUATHAN	**1. Informasi yang Wajib Disediakan dan Diumumkan Secara Berkala**					
			- Profil Kuathan	Dirjen Kuathan	Tahunan	Hardcopy/ Softcopy	1 Tahun	Perpustakaan Ditjen Kuathan
			2. Informasi yang Wajib Tersedia Setiap Saat					
			a. Santunan dan Tunjangan Cacat TNI	Dirjen Kuathan	2011	Hardcopy/ Softcopy	2 Tahun	Perubahan atas PP Nomor 56 Tahun 2007
			b. Evaluasi Dan Pengkajian Pelaksanaan Administrasi Prajurit TNI	Dirjen Kuathan	2011	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 12 Tahun 2011
			c. Pengembalian Nilai Tunai IDP bagi Prajurit TNI, Anggota Kepolisian, PNS Kemhan/Polri yang Diberhentikan Tanpa Hak Pensiun	Dirjen Kuathan	2011	Hardcopy/ Softcopy	5 Tahun	Permenhan Nomor 13 Tahun 2011
			d. Tata Cara Pengajuan Usul Gelar, Tanda Jasa dan Tanda Kehormatan Bagi Prajurit TNI dan PNS Kemhan	Dirjen Kuathan	2012	Hardcopy/ Softcopy	2 Tahun	Permenhan Nomor 01 tahun 2012
			e. Tim penelitian pusat Gelar, Tanda Jasa dan Tanda Kehormatan Bagi Prajurit TNI dan PNS Kemhan	Dirjen Kuathan	2012	Hardcopy/ Softcopy	2 Tahun	Permenhan Nomor 14 tahun 2012
			f. Pedoman Perizinan, Pengawasan dan Pengendalian Senjata Api Standar Militer di Luar Lingkungan Kemhan dan TNI	Dirjen Kuathan	2010	Hardcopy/ Softcopy	2 Tahun	Permenhan Nomor 07 tahun 2010

1	2	3	4	5	6	7	8	9
			g. Petunjuk Pelaksanaan Prosedur Perencanaan dan Penentuan Kebutuhan Materil Pertahanan Negara di Lingkungan Kemhan dan TNI	Dirjen Kuathan	2010	Hardcopy/ Softcopy	2 Tahun	Peraturan Dirjen Kuathan Nomor 01 Tahun 2010
			h. Petunjuk Pelaksanaan Prosedur Penghapusan Barang Milik Negara di Lingkungan Kemhan dan TNI	Dirjen Kuathan	2010	Hardcopy/ Softcopy	2 Tahun	Peraturan Dirjen Kuathan Nomor 02 Tahun 2010
			i. Petunjuk Pelaksanaan Tatacara Penggunaan, Pemanfaatan, Penghapusan dan Pemindahtanganan Barang Milik Negara di Lingkungan Kemhan dan TNI	Dirjen Kuathan	2010	Hardcopy/ Softcopy	2 tahun	Peraturan Dirjen Kuathan Nomor 03 Tahun 2010
			j. Pedoman Pelaksanaan Pengadaan Barang/Jasa di Lingkungan Kemhan dan TNI	Dirjen Kuathan	2011	Hardcopy/ Softcopy	Sampai dengan ada revisi	Permenhan Nomor 17 Tahun 2011
			k. Pedoman Pelaksanaan Pengadaan Alat Utama Sistem Persenjataan TNI di Lingkungan Kemhan dan TNI	Dirjen Kuathan	2011	Hardcopy/ Softcopy	Sampai dengan ada revisi	Permenhan Nomor 34 Tahun 2011
			l. Pembinaan Negara Tipe Rumah Susun di Lingkungan Kemhan dan TNI	Dirjen Kuathan	2011	Hardcopy/ Soft Copy	5 Tahun	Permenhan Nomor 03 Tahun 2011
			m. Pembinaan Rumah Negara Tipe Rusun di Lingkungan Kemhan dan TNI	Dirjen Kuathan	2011	Hardcopy/ Soft Copy	5 Tahun	Permenhan Nomor 03 Tahun 2011 Tanggal 7 Maret 2011
			n. Buku Telepon Kemhan dan TNI Tahun 2011	Dirjen Kuathan	2011	Hardcopy/ Soft Copy	5 Tahun	Kepmenhan Nomor KEP/ 761/M/X/2011 Tanggal 11 Oktober 2011
			o. Frekuensi SHF yang digunakan Kemhan dan TNI	Dirjen Kuathan	2011	Hardcopy/ Softcopy	5 Tahun	Kepmenhan Nomor KEP/ 762/M/X/2011 Tanggal 11 Oktober 2011

1	2	3	4	5	6	7	8	9
			p. Ketentuan Penggunaan Jasa Telekomunikasi di Lingkungan Kemhan dan TNI	Dirjen Kuathan	2011	Hardcopy/ Softcopy	5 Tahun	Kepmenhan Nomor KEP/ 763/M/X/2011 Tanggal 11 Oktober 2011
			q. MoU tentang Jasa Telekomunikasi	Dirjen Kuathan	2011	Hardcopy/ Softcopy	5 Tahun	MoU Nomor MoU/38/XII/ 2011 dan Nomor K.TEL.248/ HK.840/EWS-00/2011 Tanggal 2 Desember 2011 antara Kemhan dan PT. Telkom, Tbk
			r. Pedoman Pembinaan Kesehatan Matra di Lingkungan Kemhan dan TNI	Dirjen Kuathan	2011	Hardcopy/ Softcopy	5 Tahun	Kepmenhan Nomor KEP/ 904/M/XI/2011
			s. Pedoman Penyusunan Peraturan Internal Staf Medis (*Medical Staff Bylaws*) Rumah Sakit di Lingkungan Kemhan dan TNI	Dirjen Kuathan	2011	Hardcopy/ Softcopy	5 Tahun	Kepmenhan Nomor KEP/ 903/M/XI/2011
			3. Informasi yang Wajib Diumumkan Secara Serta Merta					
			a. Informasi Kegiatan Ditjen Kuathan	Dirjen Kuathan	Harian	Website	1 Tahun	Website Ditjen Kuathan
			b. Pengadaan Barang dan jasa yang bersifat umum di Ditjen Kuathan	Dirjen Kuathan	Tahunan	LPSE	1 Tahun	Website Ditjen Kuathan
			4. Informasi Terbuka Lainnya yang diminta Pemohon Informasi Pertahanan	Nihil	Nihil	Nihil	Nihil	Nihil

1	2	3	4	5	6	7	8	9
7.		BALITBANG	**1. Informasi yang Wajib Disediakan dan Diumumkan Secara Berkala**					
			a. Buletin Litbang Pertahanan	Ses Balitbang	6 bulanan	Hardcopy/ Softcopy	5 Tahun	Website Balitbang
			b. Profil Balitbang Kemhan yang meliputi Struktur Organisasi, Sejarah, tugas dan fungsi dan Rekap Personil	Ses Balitbang	Tahunan	Hardcopy/ Softcopy	1 Tahun	Website Balitbang
			c. Pengumuman Pengadaan Barang dan Jasa	Ses Balitbang	Tentatif	Hardcopy/ Softcopy	1 tahun	Website Balitbang
			2. Informasi yang Wajib Tersedia Setiap Saat					
			a. Abstraksi Hasil-Hasil Penelitian	Ses Balitbang	Tahunan	Hardcopy/ Softcopy	5 Tahun	Perpustakaan Balitbang
			b. Berita kegiatan Balitbang Kemhan	Ses Balitbang	Tentatif	Hardcopy/ Softcopy	1 Tahun	Website Balitbang
			3. Informasi yang Wajib Diumumkan Secara Serta Merta					
			- Pelaksanaan ujicoba terkait alutsista yang dapat membahayakan masyarakat sekitar daerah ujicoba seperti ujicoba Roket R-Han 122	Ses Balitbang	Tentatif	Hardcopy/ Softcopy	1 Tahun	Diumumkan ke Masyarakat Sekitar Daerah Ujicoba
			4. Informasi Terbuka Lainnya yang diminta Pemohon Informasi Pertahanan	Nihil	Nihil	Nihil	Nihil	Nihil

1	2	3	4	5	6	7	8	9
8.		BADIKLAT	**1. Informasi yang Wajib Disediakan dan Diumumkan Secara Berkala.**					
			a. Profil Badiklat Kemhan	Ses Badiklat	Tahunan	Softcopy	2 Tahun	Website Badiklat
			b. Katalog Diklat	Ses Badiklat	Tahunan	Softcopy	5 Tahun	Website Badiklat
			c. Majalah Satria	Ses Badiklat	Triwulanan	Sof copy	5 Tahun	Website Badiklat
			d. Leaflet Program Diklat Pusdiklat Badiklat Kemhan	Kapusdiklat Badiklat	Tahunan	Hardcopy/ Softcopy	5 Tahun	Website Badiklat
			2. Informasi yang Wajib Tersedia Setiap Saat					
			a. Kalender Diklat	Ses Badiklat	Tahunan	Hardcopy/ Softcopy	5 Tahun	Website Badiklat
			b. Rencana Strategis Badiklat Kemhan	Ses Badiklat	5 Tahunan	Hardcopy/ Softcopy	5 Tahun	-
			c. Petunjuk Penyelenggaraan Administrasi Pendidikan dan Pelatihan	Ses Badiklat	2011	Hardcopy/ Softcopy	5 Tahun	Website Badiklat
			d. Petunjuk Mekanisme Penyelenggaraan Pendidikan dan Pelatihan di Lingkungan Badiklat Kemhan	Ses Badiklat	2011	Hardcopy/ Softcopy	5 Tahun	Website Badiklat
			e. Petunjuk Evaluasi Penyelenggaraan Pendidikan dan Pelatihan di Lingkungan Badiklat Kemhan	Ses Badiklat	2010	Hardcopy/ Softcopy	5 Tahun	Website Badiklat
			f. Standarisasi Kurikulum Pusdiklat Jemenhan Badiklat Kemhan	Ses Badiklat	2011	Hardcopy/ Softcopy	5 Tahun	Website Badiklat
			g. Standarisasi Kurikulum Pusdiklat Bahasa Badiklat Kemhan	Ses Badiklat	2010	Hardcopy/ Softcopy	5 Tahun	Website Badiklat

1	2	3	4	5	6	7	8	9
			h. Standarisasi Kurikulum Pusdiklat Tekfunghan Badiklat Kemhan	Ses Badiklat	2010	Hardcopy/ Softcopy	5 Tahun	Website Badiklat
			i. Standarisasi Ijasah/STTP dan Sertifikat di Lingkungan Badiklat Kemhan	Ses Badiklat	2010	Hardcopy/ Softcopy	5 Tahun	Website Badiklat
			j. Pedoman pembinaan Kurikulum Diklat/Kursus di Lingkungan Badiklat Kemhan	Ses Badiklat	2010	Hardcopy/ Softcopy	5 Tahun	Website Badiklat
			k. Standarisasi Kompetensi Widyaiswara Badiklat Kemhan	Ses Badiklat	2011	Hardcopy/ Softcopy	2 Tahun	Website Badiklat
			l. Prosedur Tetap PPBK di lingkungan Badiklat Kemhan	Ses Badiklat	2010	Hardcopy/ Softcopy	5 Tahun	Website Badiklat
			3. Informasi yang Wajib Diumumkan Secara Serta Merta					
			a. Hasil Nilai test masuk jenis diklat tertentu	Kapusdiklat	Tentatif	Hardcopy/ Softcopy	1 Tahun	Sisfo Badiklat
			b. Hasil Nilai Ujian akhir jenis Diklat tertentu	Kapusdiklat	Tentatif	Hardcopy/ Softcopy	2 Tahun	Sisfo Badiklat
			4. Informasi Terbuka Lainnya yang Diminta Pemohon Informasi Pertahanan	Nihil	Nihil	Nihil	Nihil	Nihil
9.		BARANAHAN	**1. Informasi yang Wajib Disediakan dan Diumumkan Secara Berkala**					
			- Booklet Baranahan	Kabaranahan	Tahunan	Hardcopy/ Softcopy	5 Tahun	Website Kabaranahan

1	2	3	4	5	6	7	8	9
			2. Informasi yang Wajib Tersedia Setiap Saat					
			a. Revisi Pedoman Tata Cara Pelaksanaan Pembangunan dan Pemeliharaan Bangunan Dengan Cara Swakelola di Lingkungan Kemhan dan TNI	Kabaranahan	2000	Hardcopy/ Softcopy	Sampai dengan ada revisi	Surat Keputusan Menhan Nomor SKEP/949/M/ IX/2000 Tanggal 8 September 2000
			b. Pokok-Pokok Penyelenggaraan Kelaikan Komoditi Militer untuk Mendukung Pertahanan Negara	Kabaranahan	2006	Hardcopy/ Softcopy	Sampai dengan ada revisi	Permenhan Nomor PER/19/ M/XII/2006 Tanggal 19 Desember 2006
			c. Rekomendasi Perizinan untuk Produksi, Ekspor/Impor dan Agen/ Distributor Barang/Jasa Militer di Lingkungan Kemhan dan TNI	Kabaranahan	2007	Hardcopy/ Softcopy	Sampai dengan ada revisi	Permenhan Nomor PER/14/ M/XI/2007 Tanggal 6 November 2007
			d. Petunjuk Pelaksanaan Pengadaan Barang/Jasa Militer Dengan Cara Swakelola di lingkungan Kemhan dan TNI	Kabaranahan	2007	Hardcopy/ Softcopy	Sampai dengan ada revisi	Surat Keputusan Menhan Nomor SKEP/930/M/ XII/2007 Tanggal 5 Desember 2007
			e. Pokok-pokok Penyelenggaraan Kodifikasi Materiil Pertahanan Sistem Nomor Sediaan Nasional di lingkungan Kemhan dan TNI	Kabaranahan	2008	Hardcopy/ Softcopy	Sampai dengan ada revisi	Permenhan Nomor 18 Tahun 2008 Tanggal 8 Oktober 2008
			f. Pembinaan Pengadaan Materiil Pertahanan Negara di lingkungan Kemhan dan TNI	Kabaranahan	2008	Hardcopy/ Softcopy	Sampai dengan ada revisi	Permenhan Nomor 28 Tahun 2008
			g. Tata Cara Pelaksanaan Tukar Menukar Tanah dan/atau Bangunan di lingkungan Kemhan dan TNI	Kabaranahan	2009	Hardcopy/ Softcopy	Sampai dengan ada revisi	Permenhan Nomor 13 Tahun 2009

1	2	3	4	5	6	7	8	9
			h. Tata Cara Pelaksanaan Penggunaan, Pemanfaatan, Penghapusan, dan Pemindahtanganan Barang Milik Negara di lingkungan Kemhan dan TNI	Kabaranahan	2008	Hardcopy/ Softcopy	Sampai dengan ada revisi	Permenhan Nomor 29 Tahun 2009
			i. Pedoman Pelaksanaan Pengadaan Barang/Jasa di Lingkungan Kemhan dan TNI	Kabaranahan	2011	Hardcopy/ Softcopy	Sampai dengan ada revisi	Permenhan Nomor 17 Tahun 2011
			j. Pedoman Pelaksanaan Pengadaan Alat Utama Sistem Persenjataan TNI di Lingkungan Kemhan dan TNI	Kabaranahan	2011	Hardcopy/ Softcopy	Sampai dengan ada revisi	Permenhan Nomor 34 Tahun 2011
			k. Organisasi dan Tata Kerja Tim Konsultasi Pencegahan Penyimpangan Pengadaan Barang/Jasa Kemhan dan TNI	Kabaranahan	2012	Hardcopy/ Softcopy	Sampai dengan ada revisi	Permenhan Nomor 02 Tahun 2012
			3. Informasi yang Wajib Diumumkan Secara Serta Merta					
			a. Informasi yang berkaitan dengan kegiatan Badan Sarana Pertahanan Kemhan	Ses Baranahan	Update Website	Website dan media informasi lainnya	Setiap kegiatan	Website Baranahan, dan Media Informasi lainnya
			b. Pengumuman Pengadaan barang dan jasa	Ses Baranahan	-	LPSE	1 Tahun	Barang umum dan Faskon
			4. Informasi Terbuka Lainnya yang Diminta Pemohon Informasi Pertahanan	Nihil	Nihil	Nihil	Nihil	Nihil

1	2	3	4	5	6	7	8	9
10.		PUSKU	**1. Informasi yang Wajib Disediakan dan Diumumkan Secara Berkala.**					
			a. Laporan Keuangan Audited	Kapusku	Tahunan	Hardcopy/ Softcopy	1 Tahun	UU Nomor 17 Tahun 2003 dan UU Nomor 1 Tahun 2004
			b. Laporan Realisasi Anggaran	Kapusku	Tahunan	Hardcopy/ Softcopy	5 Tahun	Surat Telegram Nomor ST/ 001/2012 Tanggal 2 Januari 2012
			c. Neraca	Kapusku	Tahunan	Hardcopy/ Softcopy	5 Tahun	Surat Telegram Nomor ST/ 001/2012 Tanggal 2 Januari 2012
			d. CALK	Kapusku	Tahunan	Hardcopy/ Softcopy	5 Tahun	Surat Telegram Nomor ST/ 001/2012 Tanggal 2 Januari 2012
			2. Informasi yang Wajib Tersedia Setiap Saat.					
			a. Pedoman Pembentukan dan Pembiayaan Pokja di Lingkungan Kemhan dan TNI	Kapusku	2012	Hardcopy/ Softcopy	1 Tahun	Surat Telegram Nomor ST/001/2012 Tanggal 2 Januari 2012
			b. Besarnya ULP Organik Bagi Prajurit TNI di Lingkungan Kemhan dan TNI	Kapusku	2012	Hardcopy/ Softcopy	5 Tahun	Surat Telegram Nomor ST/16/2012 Tanggal 25 Januari 2012
			c. Penambahan Kegiatan, Digit dan Uraian Output pada Pedoman Kode Program dan Anggaran Fungsi Pertahanan TA. 2012	Kapusku	2012	Hardcopy/ Softcopy	5 Tahun	Surat Edaran Nomor SE/20/I/2012 Tanggal 30 Januari 2012
			d. Tata Cara Pembayaran Tunjangan Kinerja di Lingkungan Kemhan dan TNI	Kapusku	2012	Hardcopy/ Softcopy	5 Tahun	Surat Edaran Nomor SE/22/I/2012 Tanggal 31 Januari 2012

1	2	3	4	5	6	7	8	9
			e. Pelaksanaan Pembayaran Uang Makan bagi Pegawai Negeri Sipil di Lingkungan Kemhan dan TNI	Kapusku	2012	Hardcopy/ Softcopy	5 Tahun	Surat Edaran Nomor SE/24/II/2012 Tanggal 1 Februari 2012
			f. Kepatuhan atas Kewajiban Perpajakan	Kapusku	2012	Hardcopy/ Softcopy	5 Tahun	Surat Edaran Nomor SE/32/II/2012 Tanggal 10 Februari 2012
			g. Penyesuaian Besaran Gaji Pokok Anggota TNI dan PNS di lingkungan Kemhan dan TNI	Kapusku	2012	Hardcopy/ Softcopy	5 Tahun	Surat Edaran Nomor SE/45/II/2012 Tanggal 29 Februari 2012
			h. Pembuatan dan Pengiriman Laporan Kekuatan Personel (Bentuk KU-102) Menurut Daftar Pembayaran Penghasilan (DPP) di Lingkungan Kemhan dan TNI	Kapusku	2012	Hardcopy/ Softcopy	5 Tahun	Surat Edaran Nomor SE/49/III/2012 Tanggal 5 Maret 2012
			i. Penggunaan Komputer SAI	Kapusku	2012	Hardcopy/ Softcopy	5 Tahun	Surat Edaran Nomor SE/73/IV/2012 Tanggal 26 April 2012
			j. Petunjuk Teknis Aplikasi Komputerisasi Nota Pemindahbukuan Menteri (NPBM) Kementerian Pertahanan	Kapusku	2012	Hardcopy/ Softcopy	5 Tahun	Petunjuk Teknis Nomor Juknis/05/III/2012 Tanggal 28 Maret 2012
			3. **Informasi yang Wajib Diumumkan Secara Serta Merta**	Nihil	Nihil	Nihil	Nihil	Nihil
			4. **Informasi Terbuka Lainnya yang Diminta Pemohon Informasi Pertahanan**	Nihil	Nihil	Nihil	Nihil	Nihil

1	2	3	4	5	6	7	8	9
11.		**PUSDATIN**	1. **Informasi yang Wajib Disediakan dan Diumumkan Secara Berkala**					
			- Profil Pusdatin	Kapusdatin	2011	Softcopy	1 Tahun	Website Pusdatin
			2. **Informasi yang Wajib Tersedia Setiap Saat.**					
			a. Informasi yang berkaitan dengan tugas dan fungsi Pusdatin	Kapusdatin	2011	Softcopy	1 Tahun	Website Pusdatin
			b. Organisasi dan Tata Kerja Pusdatin	Kapusdatin	2010	Softcopy	5 Tahun	Permenhan Nomor 16 Tahun 2010 Tanggal 27 September 2010
			c. Pranata Komputer	Kapusdatin	2010	Softcopy	5 Tahun	Website Pusdatin
			d. Susunan dan Tata Kerja Jabatan Fungsional tertentu	Kapusdatin	2011	Hard Copy	5 Tahun	Permenhan Nomor 01 Tahun 2011 Tanggal 20 Januari 2011
			3. **Informasi yang Wajib Diumumkan Secara Serta Merta**					
			- Rencana Umum Pengadaan Barang & Jasa	Kapusdatin	2012	Hardcopy/ Softcopy	1 Tahun	Website LPSE Kemhan
			4. **Informasi terbuka Lainnya yang Diminta Pemohon Informasi Pertahanan.**	Nihil	Nihil	Nihil	Nihil	Nihil
12		**PUSKOM PUBLIK**	1. **Informasi yang Wajib Disediakan dan Diumumkan Secara Berkala.**					
			a. Profil Kemhan	Kapuskom Publik	Tahunan	Hardcopy/ Softcopy	2 Tahun	Website DMC Kemhan
			b. Majalah Wira	Kapuskom Publik	2 Bulanan	Hardcopy/ Softcopy	3 Tahun	Website DMC Kemhan

1	2	3	4	5	6	7	8	9
			c. Booklet	Kapuskom Publik	Tahunan	Hardcopy/ Softcopy	1 Tahun	Website DMC Kemhan
			d. Leaflet	Kapuskom Publik	6 Bulanan	Hardcopy/ Softcopy	6 Bulan	Website DMC Kemhan
			e. News Letter	Kapuskom Publik	1 Bulan	Hardcopy/ Softcopy	6 Bulan	Website DMC Kemhan
			f. Kliping Koran dan Internet	Kapuskom Publik	1 Bulan	Hardcopy	6 Bulan	Website Sisfohumas
			2. Informasi yang Wajib Tersedia Setiap Saat					
			a. Wewenang Memberikan Keterangan Pers di Lingkungan Departemen Pertahanan	Kapuskom Publik	2001	Hardcopy	Sampai ada perubahan	Kepmenhan Nomor KEP/12/ M/XI/ 2001
			b. Jabatan Fungsional Pustakawan dan Angka Kreditnya Pegawai Negeri Sipil Kemhan	Kapuskom Publik	2010	Hardcopy/ Softcopy	Sampai ada perubahan	Permenhan Nomor 05 Tahun 2010 Tanggal 31 Maret 2011
			c. Standar Layanan Informasi Pertahanan	Kapuskom Publik	2011	Hardcopy/ Softcopy	Sampai ada perubahan	Permenhan Nomor 14 Tahun 2011 Tanggal 3 Agustus 2011
			d. Pejabat Pengelola Informasi dan Dokumentasi	Kapuskom Publik	2011	Hardcopy/ Softcopy	Sampai ada perubahan	Kepmenhan Nomor KEP/614/ M/VIII/ 2011 Tanggal 15 Agustus 2011
			e. Standar Biaya Perolehan Salinan Informasi Pertahanan di lingkungan Kementrian Pertahanan	Kapuskom Publik	2012	Hardcopy/ Softcopy	Sampai ada perubahan	Kepmenhan Nomor KEP/339/M/IV/2012 Tanggal 30 April 2012
			f. Website Puskom Publik	Kapuskom Publik	2004	Hardcopy/ Softcopy	Sampai ada perubahan	-

1	2	3	4	5	6	7	8	9
			g. Wawancara dan Konferensi Pers	Kapuskom Publik	2011	Hardcopy/ Softcopy	Sampai ada perubahan	Protap/07/VI/2011/ KOMPUBLIK Tanggal 30 Juni 2011
			h. Pembuatan Press Release	Kapuskom Publik	2012	Hardcopy/ Softcopy	Sampai ada perubahan	Protap/01/VI/2012/ KOMPUBLIK
			3. Informasi yang Wajib Diumumkan Secara Serta Merta					
			- Kegiatan Kapuskom Publik	Kapuskom Publik	Tahunan	Softcopy	1 Tahun	Website DMC Kemhan
			4. Informasi Terbuka Lainnya yang Diminta Pemohon Informasi Pertahanan	Nihil	Nihil	Nihil	Nihil	Nihil
13.		PUSREHAB	**1. Informasi yang Wajib Disediakan dan Diumumkan Secara Berkala**					
			a. Majalah Warta Pusrehab	Kapusrehab	Tahunan	Hardcopy/ Softcopy	1 Tahun	-
			b. Artikel Kesehatan RS. Dr. Suyoto	Kapusrehab	Tahunan	Hardcopy/ Softcopy	1 Tahun	-
			c. Profil Pusrehab	Kapusrehab	Tahunan	Hardcopy/ Softcopy	2 Tahun	-
			d. Brosur Kegiatan Vokasional Bidrehabvok	Kapusrehab	Tahunan	Hardcopy/ Softcopy	2 Tahun	-
			e. Brosur Informasi RS. Dr. Suyoto	Kapusrehab	Tahunan	Hardcopy/ Softcopy	2 Tahun	-.

1	2	3	4	5	6	7	8	9
			2. Informasi yang Wajib Tersedia Setiap Saat					
			a. Santunan dan Tunjangan Cacat Prajurit Tentara Nasional Indonesia	Menkumham	2007	Hardcopy	5 Tahun	Peraturan Pemerintah Republik Indonesia Nomor 56 Tahun 2007 Tanggal 9 Oktober 2007
			b. Tatacara Pemberian Santunan dan Tunjangan Cacat Prajurit Tentara Nasional Indonesia	Menhan	2008	Hardcopy	5 Tahun	Peraturan Menteri Pertahanan Nomor 39 Tahun 2008
			c. Petunjuk Teknis Penyandang Cacat Prajurit Tentara Nasional Indonesia.	Panglima TNI	2009	Hardcopy	5 Tahun	Peraturan Panglima TNI Nomor Perpang 69/X/2009 Tanggal 9 Oktober 2009
			d. Penyelenggaraan Rehabilitasi Terpadu Penca/Penyandang Disabilitas Personel Pertahanan Tingkat Terampil	Kapusrehab	2011	Hardcopy	5 Tahun	Kepmenhan Nomor KEP/109/ M/II/2011 Tanggal 7 Februari 2011
			e. Visualisasi Program Rehabilitasi Terpadu	Kapusrehab	Tahunan	Hardcopy	1 Tahun	Website Pusrehab
			3. Informasi yang Wajib Diumumkan Secara Serta Merta					
			a. Kegiatan Kapusrehab Kem	Kapusrehab	Tahunan	Hardcopy	1 Tahun	Website Pusrehab
			b. Kegiatan R.S. Dr. Suyoto Pusrehab Kemhan	Kapusrehab	Tahunan	Hardcopy	1 Tahun	Website Pusrehab

1	2	3	4	5	6	7	8	9
			4. Informasi Terbuka Lainnya yang Diminta Pemohon Informasi Pertahanan	Nihil	Nihil	Nihil	Nihil	Nihil

Menteri Pertahanan,

Purnomo Yusgiantoro

Lampiran 5. Daftar Informasi Pertahanan yang Dikecualikan di Lingkungan Kementerian Pertahanan

Lampiran Keputusan Menteri Pertahanan
Nomor : KEP/1040/M/ XII/2011
Tanggal : 30 Desember 2011

DAFTAR INFORMASI PERTAHANAN YANG DIKECUALIKAN
DI LINGKUNGAN KEMENTERIAN PERTAHANAN

NO	SATKER	JENIS INFORMASI	DASAR HUKUM	BATAS WAKTU	KETERANGAN
1	2	3	4	5	6
I.	SETJEN				
	1. Biro Perencanaan	a. Kebijakan Perencanaan	1) Permenhan Nomor 14 Tahun 2011 tanggal 27 Juli 2011, Pasal 5 huruf a, huruf d, huruf e dan huruf f 2) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c	Tidak Terbatas	
		b. Rencana Strategis UO. Kemhan Tahun 2010-2014	1) Permenhan Nomor 14 Tahun 2011 tanggal 27 Juli 2011, Pasal 5 huruf a, huruf d, huruf e dan huruf f 2) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c	Tidak Terbatas	
		c. Revisi Rencana Strategis UO.Kemhan Tahun 2010 -2014	1) Permenhan Nomor 14 Tahun 2011 tanggal 27 Juli 2011, Pasal 5 huruf a, huruf d, huruf e, huruf f 2) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c	Tidak Terbatas	

1	2	3	4	5	6
		d. Rancangan Rencana Kerja UO. Kemhan	1) Permenhan Nomor 14 Tahun 2011 tanggal 27 Juli 2011, Pasal 5 huruf a, huruf d, huruf e, huruf f 2) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c	Tidak Terbatas	
		e. Rencana Kerja UO. Kemhan	1) Permenhan Nomor 14 Tahun 2011 tanggal 27 Juli 2011, Pasal 5 huruf a, huruf d, huruf e, huruf f 2) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c	Tidak Terbatas	
		f. Rencana Kerja dan Anggaran Kementerian/Lembaga.	1) Permenhan Nomor 14 Tahun 2011 tanggal 27 Juli 2011, Pasal 5 huruf a, huruf d, huruf e, huruf f 2) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c	Tidak Terbatas	
		g. Revisi Rencana Kerja dan Anggaran Kementerian/ Lembaga	1) Permenhan Nomor 14 Tahun 2011 tanggal 27 Juli 2011, Pasal 5 huruf a, huruf d, huruf e, huruf f 2) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c	Tidak Terbatas	
		h. Petunjuk Pelaksanaan Program dan Anggaran UO. Kemhan	1) Permenhan Nomor 14 Tahun 2011 tanggal 27 Juli 2011 Pasal 5 huruf a, huruf d, huruf e, huruf f	Tidak Terbatas	

1	2	3	4	5	6
			2) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c		
		i. Petunjuk Pelaksanaan Program dan Anggaran PTP Kemhan di Daerah	1) Permenhan Nomor 14 Tahun 2011 tanggal 27 Juli 2011 Pasal 5 huruf a, huruf d, huruf e, huruf f 2) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c	Tidak Terbatas	
		j. Keputusan Otorisasi Pelaksa-naan (KOP)	Permenhan Nomor 14 Tahun 2011 tanggal 27 Juli 2011 Pasal 5 huruf a, huruf d, huruf e, huruf f	Tidak Terbatas	
		k. Laporan Evaluasi Pelaksanaan Program dan Anggaran UO. Kemhan Semester I dan Tahunan	Permenhan Nomor 14 Tahun 2011 tanggal 27 Juli 2011 Pasal 5 huruf a, huruf d, huruf e, huruf f	Tidak Terbatas	
	2. Biro Kepegawaian	a. Usulan data calon pejabat yang akan memangku suatu jabatan tertentu yang diajukan dalam Baperjakat	1) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 6 ayat (3) 2) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17	Tidak Terbatas	
		b. Daftar Penilaian (Dapen) dan Daftar Penilaian Pelaksanaan Pekerjaan (DP3)	1) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 6 ayat (3)	Tidak Terbatas	

1	2	3	4	5	6
			2) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17		
		c. Proses hukum disiplin pegawai	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j	Tidak Terbatas	
		d. Dokumen proses perceraian PNS dan TNI yang mengajukan izin perceraian	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf h	Tidak Terbatas	
		e. Daftar Riwayat Hidup PNS dan TNI (Riwayat Jabatan, Pendidikan, Penugasan, Kesehatan, Keluarga)	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf h	Tidak Terbatas	
		f. Hasil evaluasi pengadaan dan penempatan CPNS	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf	Tidak Terbatas	
		g. Soal dan hasil test penerimaan CPNS, Ujian Dinas Tk. I, Ujian Penyesuaian Pangkat PNS dan seleksi calon peserta Diklatpim Tk. III	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf h		
	3. Biro Hukum	a. Surat-surat dengan klasifikasi rahasia	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf i	Tidak Terbatas	

1	2	3	4	5	6
		b. Dokumen Kontrak Pengadaan, MoU dan Perjanjian Kerjasama yang bersifat privat	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf i	Tidak Terbatas	
	4. Biro Tata Usaha	a. Hasil rapat tertutup Eselon I	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf i	Tidak Terbatas	
		b. Rapat terbatas Menhan dengan Panglima/ Kepala Staf Angkatan	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf i	Tidak Terbatas	
		c. Rapat Dengar Pendapat dan Rapat tertutup dengan Komisi I DPR RI	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf i	Tidak Terbatas	
		d. Rapat Pimpinan Kemhan RI	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf i	Tidak Terbatas	
		e. Pertemuan bilateral Menhan RI dengan Menhan negara sahabat	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf i	Tidak Terbatas	
		f. Surat-surat dengan klasifikasi rahasia	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf i	Tidak Terbatas	
		g. Surat-surat yang bersifat kebijakan	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf i	Tidak Terbatas	

1	2	3	4	5	6
	5. Biro Umum	a. Proses evaluasi dokumen Pengadaan Barang dan Jasa yang sedang berlangsung bersifat Rahasia yang boleh tahu hanya ULP atau Panitia Pengadaan sebelum diumum-kan Pemenang	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf h	Tidak terbatas	
		b. Dokumen terkait proses evaluasi Pengadaan Barang dan Jasa yang sedang berlangsung juga bersifat Rahasia yang boleh tahu hanya ULP atau Panitia Pengadaan sebelum diumumkan peme-nang	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf h	Tidak terbatas	
		c. Rincian Harga Perkiraan Sendiri (HPS) adalah bersifat Rahasia yang boleh tahu hanya PPK dan ULP/Panitia Pengadaan, karena rincian HPS untuk Acuan mengevaluasi harga penawaran dari peserta lelang	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf h	Tidak terbatas	

1	2	3	4	5	6
II.	DITJEN STRAHAN	a. Data dan informasi terkait dengan keamanan sistem informasi Ditjen Strahan, seperti : 1) Sistem Informasi Strategi Pertahanan (Sisfo Strahan) 2) Sistem Informasi Kepega-waian Ditjen Strahan (Simpeg)	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j, menjelaskan bahwa Informasi yang tidak boleh diungkapkan berdasarkan UU RI, yaitu : 1) UU RI Nomor 43 Tahun 2009 tentang Kearsipan, Pasal 44 ayat (1) menyebutkan bahwa: (1) Pencipta arsip dapat menutup akses atas arsip dengan alasan apabila dibuka untuk umum dapat mengungkapkan rahasia atau data pribadi. *(2)* UU RI Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 16 ayat (1) huruf b yaitu: a. Sepanjang tidak ditentukan lain oleh Undang-Undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut: b. Dapat melindungi ketersediaan, keutuhan, keotentikan, keraha-siaan, dan keteraksesan Informasi Elektronik dalam penyeleng-garaan Sistem Elektronik tersebut.	Tidak terbatas	

1	2	3	4	5	6
		b. Seluruh naskah perjanjian persetujuan antara Indonesia dengan negara lain dalam proses negosiasi yang dapat menimbulkan konsekuensi hukum pada pihak-pihak yang terikat atas perjanjian tersebut, ratifikasi dan sebelum diundangkan maka belum dapat dipublikasikan, seperti Nota Diplomatik dan MoU	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf f, ayat (1) dan ayat (2), bahwa : 1. Posisi, daya tawar dan stategi yang akan dan telah diambil oleh negara dalam hubungannya dengan negosiasi internasional dan 2. Korespodensi diplomatik antar negara	Sampai adanya persetujuan kedua Negara	
		c. Proses administrasi pengadaan Alutsista TNI dari luar negeri (Amerika Serikat) meliputi : 1) Pengadaan melalui FMS (*Foreign Military Sales*) seperti: (a) LOR (*Letter of Request*), (b) LOA (*Letter of Acceptance*) 2) Pengadaan melalui FMF *(Foreign Military Finance)* dalam bentuk bantuan barang/training, seperti: (a) LOR *(Letter Of Request)*, (b) LOA *(Letter Of Acceptance)*	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c, nomor 3 yaitu: 3. Jumlah, komposisi, disposisi atau lokasi kekuatan dan kemampuan dalam penyelenggaraan Sistem Pertahanan dan Keamanan Negara serta rencana pengembangannya	Sampai dengan ada kebijakan baru	

1	2	3	4	5	6
		3) Pengadaan dengan Negara lain seperti Australia, Amerika Sekikat yang melalui hibah lainnya, Contoh: *MoU, Agreement*, dll			
		d. Minimum Essential Force (MEF)	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c, nomor 3 dan nomor 4, bahwa: 3. Jumlah, komposisi, disposisi, atau lokasi kekuatan dan kemampuan dalam penyelenggaraan Sistem Pertahanan dan Keamanan Negara serta rencana pengembangannya dan 4. Gambar dan Tata tentang situasi dan keadaan pangkalan dan/ atau instalasi militer	Tidak terbatas	
		e. Doktrin Pertahanan Negara	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c, nomor 1, nomor 2, dan nomor 3 bahwa: 1. Informasi tentang stratregi, intelijen, operasional, taktik dan teknik yang berkaitan dengan penyelenggaraan Sistem Pertahanan dan Keamanan Negara, meliputi tahap perencanaan, pelaksanaan, dan pengakhiran atau evaluasi dalam kaitan dengan ancaman dari dalam dan luar negeri	Tidak terbatas	

1	2	3	4	5	6
			2. Dokumen yang memuat tentang strategi, intelijen, operasi, tekhnik dan taktik yang berkaitan dengan penyelenggaraan Sistem Pertahanan dan Keamanan Negara yang meliputi tahap perencanaan, pelaksanaan, dan pengakhiran atau evaluasi 3. Jumlah, Komposisi, Disposisi, atau Lokasi Kekuatan dan Kemampuan dalam penyelenggaraan Sistem Pertahanan dan Keamanan Negara serta rencana pengembangannya		
		f. Strategi Pertahanan Negara	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c, nomor 1, nomor 2, dan nomor 3 bahwa: 1. Informasi tentang stratregi, intelijen, operasional, taktik dan teknik yang berkaitan dengan penyelenggaraan Sistem Pertahanan dan Keamanan Negara, meliputi tahap perencanaan, pelaksanaan, dan pengakhiran atau evaluasi dalam kaitan dengan ancaman dari dalam dan luar negeri 2. Dokumen yang memuat tentang strategi, intelijen, operasi, tekhnik dan taktik yang berkaitan dengan penyelenggaraan Sistem Pertahanan dan Keamanan Negara yang meliputi tahap perencanaan, pelaksanaan, dan pengakhiran atau evaluasi		

1	2	3	4	5	6
			3. Jumlah, Komposisi, Disposisi, atau Lokasi Kekuatan dan Kemampuan dalam penyelenggaraan Sistem Pertahanan dan Keamanan Negara serta rencana pengembangannya		
		g. Postur Pertahanan Negara	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c, nomor 3 dan nomor 4, bahwa : 3. Jumlah, Komposisi, Disposisi, atau Lokasi Kekuatan dan Kemampuan dalam penyelenggaraan Sistem Pertahanan dan Keamanan Negara serta rencana pengembangannya 4. Gambar dan Tata tentang situasi dan keadaan pangkalan dan/atau instalasi militer	Tidak terbatas	
		h. Draft Kajian sebelum disahkan oleh Direktur Anstra/pejabat Contoh: 1) Studi Analisa Pengamanan NKRI dan Penanggulangan tindak terorisme 2) Implikasi perkembangan Australia terhadap Indonesia	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf f, nomor 1 dan nomor 2 bahwa: 1. Posisi, daya tawar dan strategi yang akan dan telah diambil oleh negara dalam hubungannya dengan negosiasi internasional dan 2. Korespondensi Diplomatik antar negara dan UU RI Nomor 17 Tahun 2011 tentang Intelejen Negara Bab V, Pasal 24 ayat (1) Informasi Intelejen bersifat rahasia	Sampai adanya persetujuan dan sesuai masa retensi informasi intelijen	

1	2	3	4	5	6
		3) Updating Analisa Lingkungan Strategi Kawasan Nasional, Regional, dan Global (Merupakan prediksi ancaman sehingga harus dirahasiakan yaitu Taktik dan Strategi).			
		i. Hasil Perundingan (*Record of disscussion)* dan peta-peta batas Negara di daerah perbatasan laut antara RI dengan Negara tetangga.	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf f, nomor 1 dan nomor 2, bahwa: 1. Posisi, daya tawar dan strategi yang akan dan telah diambil oleh negara dalam hubungannya dengan negosiasi internasional dan	Sampai ada persetujuan kedua negara	
		j. Hasil Perundingan (*Record of disscussion*) dan peta-peta *outstanding boundary* problem (OBP) di daerah perbatasan darat antara RI dengan Negara tetangga.	2. Korespondensi diplomatik antar negara		
		k. Pengerahan Komponen Hanneg meliputi : 1) MoU pengamanan Obyek Vital (Kemhan - BP Migas, Kemhan - East Natuna). 2) Perpres, Permen tentang Penugasan Kongo ke wilayah konflik (Haiti, Kongo, Libanon, dll	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c, nomor 3, bahwa: 3. Jumlah, komposisi, disposisi atau lokasi kekuatan dan kemampuan dalam penyelenggaraan Sistem Pertahanan dan Keamanan negara serta rencana pengembanganya	Sampai ada kebijakan baru	

1	2	3	4	5	6
		l. Regulasi yang terkait dengan pelaksanaan operasi militer	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c	Sampai Operasi Militer dinyatakan selesai	
		m. Disposisi yang dinyatakan rahasia oleh pimpinan	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c	Sampai dinyatakan tidak rahasia oleh pimpinan	
		n. Regulasi yang karena sifatnya dinyatakan rahasia	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c	Sampai dilakukan pengundangan terhadap regulasi tersebut	
III.	DITJEN RENHAN	a. Rencana Strategis: Lampiran tentang data rencana belanja/ pembelian/Alutsista/peralatan dan *shopping list.*	Kerahasiaan kekuatan militer/keamanan Negara	Selamanya	
		b. Rencana Kerja: Lampiran tentang kekuatan, kemampuan dan gelar	1) Kerahasiaan kekuatan militer/keamanan Negara 2) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf i bahwa memorandum atau surat-surat antar Badan Publik atau intra Badan Publik, yang menurut sifatnya dirahasiakan kecuali atas putusan Komisi Informasi atau pengadilan	5 Tahun	

1	2	3	4	5	6
		c. *Exercise*/perhitungan RAPBN Kementerian (sebelum disampaikan, dibahas DPR) d. Rincian rencana alokasi anggaran (termasuk pembukuannya)	1) UU RI Nomor 17 Tahun 2003 tentang Keuangan Negara, Pasal 30 ayat (1) dan (2), bahwa: (1) Presiden menyampaikan Rancangan Undang Undang tentang pertanggu-ngjawaban pelaksanaan APBN kepada DPR berupa laporan keuangan yang telah diperiksa oleh Badan Pemeriksa Keuangan selambat-lambatnya 6 (enam) bulan setelah Tahun anggaran berakhir (2) Laporan keuangan dimaksud setidak-tidaknya meliputi Laporan Realisasi APBN, Neraca, Laporan Arus Kas dan Catatan atas Laporan Keuangan, yang dilampiri dengan laporan keuangan perusahaan Negara dan badan lainnya. 2) UU RI Nomor 15 Tahun 2004 tentang Pemeriksaan Pengelolaan dan Tanggung Jawab Keuangan Negara tertera pada: (a) Pasal 17 (b) Pasal 18 ayat (1) dan ayat (2) dan (c) Pasal 19 ayat (1) dan ayat (2)	5 Tahun	

1	2	3	4	5	6
		e. Rancangan dan/atau surat-surat yang mempunyai klasifikasi sifat rahasia	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf i bahwa memorandum atau surat-surat antar Badan Publik atau intra Badan Publik, yang menurut sifatnya dirahasiakan kecuali atas putusan Komisi Informasi atau pengadilan		Sesuai perkembangan
		f. Lembar Kerja (LK) Rencana Kerja dan Anggaran RKA-KL Kemhan dan TNI dan Daftar Isian Pelaksanaan Anggaran (DIPA) Kemhan dan TNI	1) UU RI Nomor 17 Tahun 2003 tentang Keuangan Negara, tertera pada: (a) Pasal 11 ayat (5) menjelaskan bahwa "Belanja negara dirinci menurut organisasi, fungsi, dan jenis belanja" dan (b) Pasal 15 ayat (5) menjelaskan bahwa "APBN yang disetujui oleh DPR terinci sampai dengan unit organisasi, fungsi, program, kegiatan dan jenis belanja" 2) PP Nomor 90 Tahun 2010 tentang Rencana Kerja dan Anggaran Kementerian Negara/ Lembaga sebagai pengganti PP Nomor 21 Tahun 2004 dijelaskan dalam Pasal 5 dan Pasal 6 adalah UU Nomor 14 Tahun 2008 tentang keterbukaan informasi Publik pada Pasal 17 tentang Informasi yang Dikecualikan antara lain pada huruf c.	5 Tahun	

1	2	3	4	5	6
		g. Rencana Pembangunan MEF, terkait dengan jenis Alutsista (Spektek)		15 Tahun	3 Renstra
		h. Rencana Dukungan Anggaran Pelaksanaan Kegiatan Operasi TNI		20 Tahun	
		i. Dokumen pertanggungjawaban penerbitan otorisasi (KOM)	1) UU RI Nomor 17 Tahun 2003 tentang Keuangan Negara 2) UU RI Nomor 1 Tahun 2004 tentang Perbendaharaan Negara bahwa dokumen pertanggungjawaban (KOM, BA dan SPP) bersifat terbatas dan hanya diketahui dan digunakan oleh instansi tertentu/terkait 3) SKB Menkeu dan Menhan Nomor 630/KMK06/2004	Tidak Terbatas	Selama KOM sebagai alat pelaksanaan anggaran
		j. Dokumen pertanggungjawaban berita acara anggaran terpusat LTGA dan BMP		5 Tahun	
		k. Dokumen pertanggungjawaban SPP Anggaran terpusat LTGA dan BMP	Dokumen-dokumen PHLN dan PDN hanya diketahui instansi tertentu kerena menyangkut kekuatan Alutsista	10 Tahun	

1	2	3	4	5	6
		l. Dokumen pertanggung jawaban Pinjaman, Hibah Luar Negeri (PHLN), Pin-jaman Dalam Negeri (PDN), Rupiah murni pendamping		20 Tahun	
		m. Laporan Evaluasi Pelaksa-naan Program dan Anggaran Pertahanan Negara	1) UU RI Nomor 17 Tahun 2003 tentang Keuangan Negara Pasal 30 Ayat 1 dan 2 2) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara RI Nomor 4846)	5 Tahun	
IV.	DITJEN POTHAN	a. Bela Negara, terdiri dari: 1) Lingkungan Pemukiman 2) Lingkungan Pekerjaan 3) Lingkungan Pendidikan	1) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 yang menyatakan Informasi yang dapat membahayakan pertahanan dan keamanan Negara 2) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c, nomor 3, menjelaskan bahwa: 3. Jumlah, komposisi, disposisi atau dislokasi kekuatan dan kemampuan dalam penyelenggaraan	TidakTerbatas	

1	2	3	4	5	6
		b. Komponen Cadangan, yaitu: 1) Matra Darat 2) Matra Laut 3) Matra Udara	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c, nomor 3, menjelaskan bahwa: 3. Jumlah, komposisi, disposisi atau dislokasi kekuatan dan kemampuan dalam penyelenggaraan	Tidak terbatas	
		c. Komponen Pendukung terdiri dari: 1) Komponen SDM 2) Komponen SDAB 3) Komponen SARPRAS	1) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, yang apabila dibuka dan diberikan kepada pemohon informasi publik dapat mengungkapkan kekayaan alam Indonesia 2) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c nomor 3, menjelaskan bahwa: 3. Jumlah, komposisi, disposisi atau dislokasi kekuatan dan kemampuan dalam penyelenggaraan sistem pertahanan dan keamanan negara serta rencana pengembangannya	Tidak terbatas	
		d. Data Direktorat Teknologi Industri Pertahanan, terdiri atas: Industri Alutsista, Industri Non Alutsista, Industri Pendukung Litbang, Lembaga Uji, Lembaga pendidikan (Perguruan tinggi, politeknik, Sekolah Kejuruan)	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c nomor 3, menjelaskan bahwa: 3. Jumlah, komposisi, disposisi atau dislokasi kekuatan dan kemampuan dalam penyelenggaraan sistem pertahanan dan keamanan negara serta rencana pengembangannya	Tidak terbatas	
		e. Data Direktorat Veteran, terdiri atas: Data veteran pejuang kemerdekaan RI, Data veteran pembela kemerdekaan RI, Data veteran perdamaian	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c nomor 3, menjelaskan bahwa: 3. Jumlah, komposisi, disposisi atau dislokasi kekuatan dan kemampuan dalam penyelenggaraan sistem pertahanan dan keamanan negara serta rencana pengembangannya	Tidak terbatas	
V	DITJEN KUATHAN	a. Keputusan Menteri Pertahanan tentang Alokasi Penyediaan Prajurit TNI	1) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c nomor 3 2) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j	Sampai terbitnya keputusan baru	
		b. Rekapitulasi Kekuatan Prajurit TNI	1) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c nomor 3 2) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j	Tidak terbatas	
		c. Data kondisi nyata tentang Rekapitulasi Alutsista dan Non Alutsista	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c nomor 3	Tidak terbatas	

1	2	3	4	5	6
		d. Kemampuan Alutsista TNI dan Non Alutsista TNI yang tergelar	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c nomor 3	Tidak terbatas	
		e. Daftar alokasi, database penggunaan frekuensi untuk keperluan pertahanan negara	1) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c nomor 3	Tidak terbatas	
			2) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j		
VI	ITJEN	a. Dokumen Hasil Pengawasan Pemeriksaan Fungsi Manajerial, Fungsi Teknis dan Fungsi Organik terdiri dari : 1) Pernyataan Hasil Pemeriksaan 2) Laporan Hasil Pemeriksaan 3) Intisari Laporan Hasil Pemeriksaan 4) Pernyataan Penutupan Hasil Pemerikasaan 5) Tindak Lanjut Hasil Pemerikasaan	1) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf i 2) Peraturan Menpan Nomor PER/04/M.PAN/03/2008 tentang Standar Audit Pengawasan Pemerintah	Tidak terbatas	

1	2	3	4	5	6
		b. Database Aplikasi Sisfo Itjen, *E-Filling System*	1) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik Pasal 17 huruf i 2) UU RI Nomor 30 Tahun 2000 tentang Rahasia Dagang, Pasal 1 3) UU RI Nomor 43 Tahun 2009 tentang Kersipan, Pasal 44 ayat (1)	Tidak terbatas	
		c. Salinan Dokumen Format Pengumuman Tambahan Berita Negara LHKPN (Laporan Harta Kekayaan Penyelenggara Negara) Seluruh Pejabat di Lingkungan Kemhan	1) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j informasi yang tidak boleh diungkapkan berdasarkan UU RI, yaitu: a) UU RI Nomor 8 Tahun 1981 tentang Hukum Acara Pidana, Pasal 322 ayat (1) menyebutkan bahwa barang siapa dengan sengaja membuka rahasia yang wajib disimpannya karena jabatan atau pencaharriannya, baik yang sekarang maupun yang dahulu, diancam dengan pidana penjara paling lama sembilan bulan atau pidana denda paling banyak sembilan ribu rupiah b) UU RI Nomor 43 Tahun 2009 tentang kearsipan, khususnya Pasal 44 ayat (1) huruf h menyebutkan, bahwa pencipta arsip dapat menutup akses atas arsip dengan alasan apabila dibuka untuk umum, dapat	Tidak terbatas	

1	2	3	4	5	6
			mengungkap rahasia atau data pribadi a) Keputusan Ketua Komisi Pemberantasan Korupsi Nomor KEP.07/KPK/02/2005 tentang Tata cara Pendaftaran, Pengumuman dan Pemeriksaan Laporan Harta Kekayaan Penyelenggaraan Negara (LHKPN) yaitu: (1) Pasal 3 ayat (2) menjelaskan bahwa Surat Pernyataan dan Surat Kuasa yang menjadi bagian yang tidak terpisahkan dari LHKPN ditandatangani oleh penyelenggara negara yang bersangkutan diatas materai sesuai dengan ketentuan (2) Pasal 5 ayat (1) menjelaskan bahwa Pengumuman LHKPN dilakukan setelah LHKPN diterima KPK dan dilakukan verifikasi (3) Pasal 5 ayat (2) Pengumuman Kekayaan sebagaimana dimaksud dalam ayat (1) dilakukan sebelum, selama dan setelah penyelenggara negara menjabat dengan cara mengumumkan LHKPN kepada publik melalui		

1	2	3	4	5	6
			Berita Negara Republik Indonesia/ Tambahan Berita Negara dan atau Media lain yang ditetapkan oleh KPK (4) Pasal 5 ayat (4) menjelaskan bahwa Pelaksanaan Pengumuman LHKPN dilakukan oleh penyelenggara negara yang bersangkutan dan atau oleh KPK berdasarkan Surat Kuasa yang diberikan penyelenggara negara kepada KPK (5) Pasal 5 ayat (5) Pengumuman harta kekayaan yang diumumkan oleh penyenyelenggara negara yang bersangkutan dilaksanakan melalui Berita Negara Republik Indonesia/Tambahan Berita Negara dan atau melalui koran harian nasional atau harian lokal ditingkat Kabupaten dan atau Provinsi dimana penyelenggara negara berdomisili atas biaya penyelenggara yang bersangkutan dengan menggunakan format pengumuman yang telah ditetapkan oleh KPK dalam waktu selambat-lambatnya 30 (tiga puluh) hari kerja setelah LHKPN dinyatakan lengkap oleh KPK		

1	2	3	4	5	6
			(6) Pasal 5 ayat (6) menjelaskan bahwa Bukti salinan atau fotokopi pengumuman Harta Kekayaan Penyelenggara Negara disampai-kan kepada KPK selambat-lambatnya 30 (tiga puluh) hari kerja terhitung tanggal diumumkan oleh Penyelenggara Negara yang bersangkutan (7) Pasal 5 ayat (7) menjelaskan bahwa untuk Kepentingan Publik Akuntabilitas dan Transparansi, KPK membuka akses informasi LHKPN yang telah diumumkan kepada publik dengan syarat-syarat akses informasi yang ditetapkan oleh KPK		
VII	BALITBANG	a. Naskah lengkap hasil penelitian yang terkait dengan Alutsista dan kajian strategis antara lain Postur Pertahanan, Doktrin dan Sismed	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c: Informasi publik yang apabila dibuka dan diberikan kepada pemohon informasi publik dapat membahayakan pertahanan dan keamanan negara	Tidak terbatas	
		b. Penelitian, Pengembangan dan/ atau Penerapan (Litbangrap) Iptek yang berisiko tinggi dan berbahaya	1) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 a) huruf b: informasi publik apabila dibuka dan diberikan kepada Pemohon Informasi Publik dapat	Selama hasil kajian belum diproduksi secara massal	

1	2	3	4	5	6
			mengganggu kepentingan perlindung-an hak atas kekayaan intelektual dan perlindungan dari persaingan usaha tidak sehat b) huruf c : Informasi publik yang apabila dibuka dan diberikan pemohon informasi publik dapat membahayakan pertahanan dan keamanan negara 2) UU RI Nomor 18 Tahun 2002 tentang Sistem Nasional Litbangrap Iptek Pasal 22 ayat (2) untuk melaksanakan ketentuan sebagaimana dimaksud dalam ayat (1), pemerintah mengatur perizinan bagi pelaksanaan kegiatan penelitian, pengembangan, dan penerapan ilmu pengetahuan dan teknologi yang berisiko tinggi dan berbahaya dengan memperhatikan standar nasional dan ketentuan yang berlaku secara internasional 3) PP Nomor 48 Tahun 2009 tentang Perijinan Pelaksanaan Kegiatan Litbangrap Iptek yang berisiko tinggi dan berbahaya, merupakan penjabaran dari Pasal 22 ayat (3) UU RI Nomor 18 Tahun 2002		

1	2	3	4	5	6
		c. Spesifikasi standar tipe Alutsista hasil Litjianbang	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 1) huruf b: informasi publik apabila dibuka dan diberikan kepada Pemohon Informasi Publik dapat mengganggu kepentingan perlindungan hak atas kekayaan intelektual dan perlindungan dari persaingan usaha tidak sehat 2) huruf c: Informasi publik yang apabila dibuka dan diberikan pemohon informasi publik dapat membahayakan pertahanan dan keamanan negara	Tidak terbatas	
		d. Komposisi Material/Raw Material Hasil Litjianbang dan Formula Rumusan Kimia yang berkaitan dengan Alutsista	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 1) huruf b: informasi publik apabila di buka dan diberikan kepada Pemohon Informasi Publik dapat mengganggu kepentingan perlindungan hak atas kekayaan intelektual dan perlindungan dari persaingan usaha tidak sehat 2) huruf c : Informasi publik yang apabila di buka dan diberikan pemohon informasi publik dapat membahayakan pertahanan dan keamanan negara	Tidak terbatas	
		3) Desain dan rancang bangun hasil Litjianbang	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 1) huruf b: informasi publik apabila dibuka	Tidak terbatas	

1	2	3	4	5	6
			dan diberikan kepada Pemohon Informasi Publik dapat mengganggu kepentingan perlindungan hak atas kekayaan intelektual dan perlindungan dari persaingan usaha tidak sehat 2) huruf c: Informasi publik yang apabila dibuka dan diberikan pemohon informasi publik dapat membahayakan pertahanan dan keamanan negara		
		4) Kerjasama dengan pihak lain baik di dalam maupun luar negeri dibidang Litbang terkait dengan kesepakatan perjanjian tentang Kerahasian data dan hasil Litbang	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 1) huruf b: informasi publik apabila dibuka dan diberikan kepada Pemohon Informasi Publik dapat mengganggu kepentingan perlindungan hak atas kekayaan intelektual dan perlindungan dari persaingan usaha tidak sehat 2) huruf c: Informasi publik yang apabila di buka dan diberikan pemohon informasi publik dapat membahayakan pertahanan dan keamanan negara	Tidak terbatas	
VIII	BADIKLAT	a. Laporan keuangan dan dokumen pendukung yang belum diaudit	1) UUD Tahun 1945 Pasal 4 ayat (1) 2) UU RI Nomor 1 Tahun 2004 tentang Perbendaharaan Negara	Sampai diaudit dan mendapat persetujuan pimpinan	

1	2	3	4	5	6
			3) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j informasi yang tidak boleh diungkapkan berdasarkan UU RI		
		b. Pengadaan Barang dan Jasa yang meliputi kegiatan sebagai berikut: Proses Evaluasi dukumen pengadaan barang dan jasa yang sedang berlangsung, Dokumen yang terkait dengan pengadaan Barang dan Jasa yang sedang berlangsung, Rincian Harga Perkiraan Sendiri (HPS), Perjanjian Kontrak Pengadaan Barang dan Jasa (KPBJ)	1) UUD Tahun 1945 Pasal 4 ayat (1) 2) UU RI Nomor 1 Tahun 2004 tentang Perbendaharaan Negara 3) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j 4) Perpres 54 Tahun 2010 tentang Pengadaan Barang dan Jasa	Tidak terbatas	
		c. Kurikulum Diklat yang belum disahkan masih dalam penyusunan dan perumusan d. Nilai Akhir Peserta Diklat yang belum disahkan, catatan Personel, peserta Diklat selama mengikuti pendidikan, nilai Akhir peserta Diklat yang belum disahkan	1) UU RI Nomor 43 Tahun 2009 tentang Kearsipan, Pasal 44 ayat (1), menjelaskan bahwa: (1) Pencipta arsip dapat menutup akses atas arsip dengan dengan apabila arsip dibuka untuk umum dapat: b. mengganggu kepentingan pelindungan hak atas kekayaan intelektual dan pelindungan dari persaingan usaha tidak sehat	Sampai disahkan dan mendapat persetujuan pimpinan	

1	2	3	4	5	6
			2) UU RI Nomor 43 Tahun 2009 tentang Kearsipan, Pasal 44 ayat (1) menjelaskan bahwa: (1) Pencipta arsip dapat menutup akses atas arsip dengan alasan apabila dibuka untuk umum dapat mengungkapkan rahasia atau data pribadi		
		e. Rencana Masterplan Pengembangan IT Badiklat Kemhan yang meliputi kegiatan: Pengembangan Aplikasi Internal, Design Arsitektur Jaringan, Sistem Keamanan Jaringan dan Database aplikasi Sisfo Badiklat	1) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j, menjelaskan bahwa Informasi yang tidak boleh diungkapkan 2) UU RI Nomor 30 Tahun 2000 tentang Rahasia Dagang, Pasal 1 menyebutkan Rahasia Dagang adalah informasi yang tidak diketahui oleh umum di bidang teknologi dan/ atau bisnis, mempunyai nilai ekonomi karena berguna dalam kegiatan usaha, dan dijaga kerahasiaannya oleh pemilik Rahasia Dagang 3) UU RI Nomor 43 Tahun 2009 tentang Kearsipan, Pasal 44 ayat (1), menjelaskan bahwa: (1) Pencipta arsip dapat menutup akses atas arsip dengan dengan apabila arsip dibuka untuk umum dapat:	Tidak Terbatas	

1	2	3	4	5	6
			b. Mengganggu kepentingan pelindungan hak atas kekayaan intelektual dan pelindungan dari persaingan usaha tidak sehat 4) UU RI Nomor 43 Tahun 2009 tentang Kearsipan, Pasal 44 ayat (1) menjelaskan bahwa: (1) Pencipta arsip dapat menutup akses atas arsip dengan alasan apabila dibuka untuk umum dapat mengungkapkan rahasia atau data pribadi 5) UU RI Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 16 ayat (1) huruf b, menjelaskan bahwa: (1) Sepanjang tidak ditentukan lain oleh undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut: b. Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut		

1	2	3	4	5	6
IX	BARANAHAN	a. Pengadaan Barang dan Jasa : 1) Dokumen yang terkait dengan pengadaan barang dan jasa yang sedang berlangsung 2) Harga Perkiraan Sendiri (HPS) 3) Perjanjian Kontrak pengadaan barang jasa	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j	Tiap Tahun	
		b. Data, Lokasi dan Spesifikasi Teknis Alutsista	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c	Tidak Terbatas	
		c. Database anggota yang sedang melaksanakan sertifikasi kelaikan	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf h nomor 4	Tidak Terbatas	
		d. Database Alutsista yang dalam proses sertifikasi	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c	Tidak Terbatas	
		e. Database Kodifikasi Materiil untuk kepentingan Pertahanan Negara	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c	Tidak Terbatas	
		f. Dokumen yang terkait dengan Identifikasi materiil proses kodifikasi	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf b	Tidak Terbatas	

1	2	3	4	5	6
		g. Referensi kodifikasi yang terkait dengan bahan kerja Puskod yang berkaitan dengan hak cipta	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j	Tidak Terbatas	
X	PUSKU	a. Database Sistem Akuntansi Instansi (SAI) dan Iuran Wajib Pegawai (IWP)	1) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j, menjelaskan bahwa Informasi yang tidak boleh diungkapkan 2) UU RI Nomor 30 Tahun 2000 tentang Rahasia Dagang, Pasal 1 menjelaskan bahwa Rahasia Dagang adalah informasi yang tidak diketahui oleh umum di bidang teknologi dan/atau bisnis, mempunyai nilai ekonomi karena berguna dalam kegiatan usaha, dan dijaga kerahasiaannya oleh pemilik Rahasia Dagang 3) UU RI Nomor 43 Tahun 2009 tentang Kearsipan, Pasal 44 ayat (1), menjelaskan: (1) Pencipta arsip dapat menutup akses atas arsip dengan apabila arsip dibuka untuk umum dapat mengganggu kepentingan pelindungan hak atas kekayaan intelektual dan pelindungan dari persaingan usaha tidak sehat	Tidak Terbatas	

1	2	3	4	5	6
		b. Pengadaan Barang dan Jasa : 1) Proses Evaluasi dokumen pengadaan barang dan jasa yang sedang berlangsung 2) Dokumen yang terkait dengan pengadaan barang dan jasa yang sedang berlangsung 3) Rincian Perkiraan Sendiri (HPS) 4) Perjanjian kontrak pengadaan barang dan jasa	1) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j, menjelaskan bahwa informasi yang tidak boleh diungkapkan berdasarkan UU RI 2) Perpres 54 Tahun 2010 tentang Pengadaan barang dan jasa	Tidak Terbatas	
		c. Risalah rapat internal pimpinan yang menyangkut kebijakan yang bersifat rahasia berikut dokumen pendukungnya	1) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j menjelaskan bahwa informasi yang tidak boleh diungkapkan berdasarkan UU RI 2) UU Nomor 43 Tahun 2009 tentang Kearsipan, khususnya Pasal 44 ayat (1) huruf i menjelaskan bahwa mengungkap memorandum atau surat-surat yang menurut sifatnya perlu dirahasiakan	Tidak Terbatas	

1	2	3	4	5	6
		d. Dokumen penarikan dana ke Kantor Pelayanan Pembendaharaan Negara (KPPN) berupa Surat Perintah Membayar (SPM) dan Surat Perintah Pencairan Dana (SP2D) dan seperti: 1) Dokumen Pertangungjawaban penyaluran Dana Nota Pindah Bukuan Menteri (NPBM) 2) Dokumen pertangungjawaban Berita Acara Anggaran Terpusat Listrik Telepon Gas Air (LTGA) dan Bahan Minyak Pelumas (BMP) 3) Dokumen pertangungjawaban SPP Anggaran Terpusat Listrik Telepon Gas Air (LTGA) dan Bahan Minyak Pelumas (BMP) 4) Laporan realisasi Penyaluran Nota Pindah Bukuan Menteri	1) UU RI Nomor 17 Tahun 2003 tentang Keuangan Negara 2) UU RI Nomor 1 Tahun 2004 tentang Perbendaharaan Negara 3) Dokumen-dokumen pertanggungjawaban keuangan PHLN dan PDN hanya instansi tertentu karena menyangkut kekuatan Alutsista	Tidak Terbatas	

1	2	3	4	5	6
		5) Dokumen pertanggungjawaban keuangan Pinjaman Hibah Luar Negeri (PHLN), Pinjaman Dalam Negeri (PDN), Rupiah Murni Pendamping e. Laporan Keuangan Kemhan beserta dokumen pendukungnya	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j, menjelaskan bahwa informasi yang tidak boleh diungkapkan berdasarkan UU RI yaitu : 1) UU RI Nomor 17 Tahun 2003 tentang Keuangan Negara, Pasal 30 ayat (1) dan ayat (2), sebagai berikut: (1) Presiden menyampaikan Rancangan UU RI tentang pertanggungjawaban pelaksanaan APBN kepada DPR berupa laporan keuangan yang telah diperiksa oleh Badan Pemeriksa Keuangan, selambat-lambatnya 6 (enam) bulan setelah Tahun anggaran berakhir (2) Laporan keuangan dimaksud setidak-tidaknya meliputi Laporan Realisasi APBN, Neraca, Laporan Arus Kas, dan Catatan atas Laporan Keuangan, yang dilampiri dengan laporan keuangan perusahaan Negara dan badan lainnya	Tidak Terbatas	

1	2	3	4	5	6
			2) UU RI Nomor 15 Tahun 2004 tentang Pemeriksaan Pengelolaan dan Tanggung Jawab Keuangan Negara (a) Pasal 17 ayat (1) (b) Pasal 18 ayat (1) dan (2) (c) Pasal 19 ayat(1) dan (2)		
XII	PUSDATIN	a. Daftar alokasi *bandwidth* dan penggunaan *bandwidth* untuk keperluan sistem informasi pertahanan negara (sisfohan-neg)	1) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf c, menjelaskan bahwa informasi publik yang apabila dibuka dan diberikan kepada pemohon informasi publik dapat membahayakan pertahanan dan keamanan negara	Tidak terbatas	
			2) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j		
		b. Database sisfohanneg	1) UU Nomor 30 Tahun 2000 tentang Rahasia Dagang, Pasal 1 menjelaskan bahwa Rahasia Dagang adalah informasi yang tidak diketahui oleh umum di bidang teknologi dan/atau bisnis, mempunyai nilai ekonomi karena berguna dalam kegiatan usaha, dan dijaga kerahasiaannya oleh pemilik Rahasia Dagang	Tidak terbatas	

1	2	3	4	5	6
			UU RI Nomor 43 Tahun 2009 tentang Kearsipan, Pasal 44 ayat (1) huruf b, menjelaskan bahwa: (1) Pencipta arsip dapat menutup akses atas arsip dengan dengan apabila arsip dibuka untuk umum dapat : b. mengganggu kepentingan pelin-dungan hak atas kekayaan intelektual dan pelindungan dari persaingan usaha tidak sehat		
		c. Laporan penyelenggaraan sisfohanneg yang berklasifikasi rahasia	1) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 6 ayat (3) huruf b, menjelaskan bahwa: (3) Informasi publik yang tidak dapat diberikan oleh Badan Publik, sebagaimana dimaksud pada ayat (1) adalah: b. Informasi yang berkaitan dengan kepentingan perlin-dungan usaha dari persaingan usaha tidak sehat	Tidak terbatas	
			2) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf b		
			3) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j		

1	2	3	4	5	6
		d. Proses dan hasil monitoring dan evaluasi penyele-nggaraan sisfohanneg	1) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 6 ayat (3) huruf b, menjeaskan bahwa: (2) Informasi publik yang tidak dapat diberikan oleh Badan Publik, sebagaimana dimaksud pada ayat (1) adalah: b. Informasi yang berkaitan dengan kepentingan perlin-dungan usaha dari persaingan usaha tidak sehat 2) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf b 3) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j	Tidak terbatas	
		c. Daftar penomoran pengguna jaringan komunikasi data sisfohanneg	1) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 6 ayat (3) huruf b, menjeaskan bahwa: (3) Informasi publik yang tidak dapat diberikan oleh Badan Publik, sebagaimana dimaksud pada ayat (1) adalah: b. Informasi yang berkaitan dengan kepentingan perlindungan usaha dari persaingan usaha tidak sehat	Tidak terbatas	

1	2	3	4	5	6
			2) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf b 3) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j		
		f. Lokasi dan konfigurasi data *center, disaster recovery center,* database dan aplikasi serta *username dan password*	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j	Tidak terbatas	
		g. Arsitektur infrastruktur jaringan komunikasi data	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j, yaitu: 1) UU RI Nomor 43 Tahun 2009 tentang Kearsipan, Pasal 44 ayat (1) menyebutkan bahwa (1) Pencipta arsip dapat menutup akses atas arsip dengan alasan apabila dibuka untuk umum dapat mengungkapkan rahasia atau data pribadi 2) UU RI Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 16 ayat (1) huruf b, menjelaskan bahwa:	Tidak terbatas	

1	2	3	4	5	6
			(1) Sepanjang tidak ditentukan lain oleh undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut: b. Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut		
		h. Data dan informasi terkait dengan keamanan sistem informasi	UU RI Nomor Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j, yaitu: 1) UU Nomor 43 Tahun 2009 tentang Kearsipan, Pasal 44 ayat (1) menjelaskan bahwa: (1) Pencipta arsip dapat menutup akses atas arsip dengan alasan apabila dibuka untuk umum dapat mengungkapkan rahasia atau data pribadi 2) UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 16 ayat 1 huruf b	Tidak terbatas	

1	2	3	4	5	6
		i. Informasi identitas dan konten layanan sisfohanneg	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j	Tidak terbatas	
		j. Sistem Persandian Pertahanan	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 perihal Sistem Persandian tertera dalam: 1) Huruf c nomor 6 2) Huruf f nomor 3	Tidak terbatas	
XII	PUSKOM PUBLIK	a. Berita bersifat tertutup/ rahasia yang disampaikan pejabat Kemhan Eselon I ke atas	UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17 huruf j	Tidak terbatas	
		b. Hasil liputan rapat tertutup di Kemhan, MPR/ DPR RI	UU RI Nomor 43 Tahun 2009 tentang Kearsipan khususnya Pasal 44 ayat (1) huruf i, yang menjelaskan bahwa: (1) mengungkapkan memorandum atau surat-surat yang bersifat rahasia perlu dirahasiakan	Tidak terbatas	
XIII	PUSREHAB	a. Data rekam medis terdiri atas identitas pasien, riwayat dan diagnosis penyakit, data penunjang medis, tindakan medis/pengobatan, resume medis	Permenkes Nomor : 269/Menkes/PER/III/ 2008	Tidak Tebatas	

1	2	3	4	5	6
		b. Data Penyandang Cacat Personel Pertahanan	1) UU RI Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia 2) Peraturan Pemerintah RI Nomor 56 Tahun 2007 tentang Santunan dan Tunjangan Cacat TNI 3) UU RI Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 17	Tidak terbatas	

Menteri Pertahanan,

Purnomo Yusgiantoro