



UNIVERSITAS PERTAHANAN REPUBLIK INDONESIA

DISERTASI

**STRATEGI PENGEMBANGAN KEBIJAKAN KEDAULATAN
PERTAHANAN SIBER NASIONAL GUNA MENGHADAPI
BERBAGAI ANCAMAN PERTAHANAN NEGARA**

Richardus Eko Indrajit

NIM. 220190201016

FAKULTAS STRATEGI PERTAHANAN

PROGRAM STUDI DOKTORAL


COHORT 2

SENTUL

2021

LEMBAR PERSETUJUAN UJIAN TERBUKA

Nama : **Richardus Eko Indrajit**
NIM : **220190201016**
Program Studi : **Ilmu Pertahanan**
Fakultas : **Strategi Pertahanan**
Judul Disertasi : **Strategi Pengembangan Kebijakan Kedaulatan Pertahanan Siber Nasional Guna Menghadapi Berbagai Ancaman Pertahanan Negara**

Promotor,


Laksamana TNI (Purn) Prof. Dr. Marsetio, M.M.

Co-Promotor 1,



**Kolonel Sus Dr. Ir. Rudy
AG Gultom, MSc.**

Tanggal: Oktober 2021

Co-Promotor 2,



**Brigjen TNI Dr. Pujo Widodo, S.E.,
M.A., MDS, M.Si., M.Si. (Han)**

Tanggal: Oktober 2021

Mengetahui,

Plh. Direktur Program Doktoral,

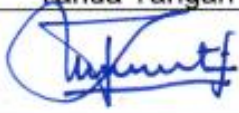





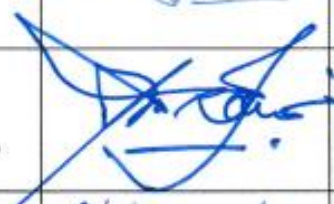




Mayjen TNI Dr. Joni Widjayanto, S.Sos., M.M., CIQnR, CIQaR

Tanggal: Oktober 2021

LEMBAR PENGESAHAN DISERTASI

Nama : Richardus Eko Indrajit
NIM : 220190201016
Program Studi : Doktoral Ilmu Pertahanan | Cohort 2
Konsentrasi : Strategi Pertahanan
Judul Disertasi : Strategi Pengembangan Kebijakan Kedaulatan
Pertahanan Siber Nasional Guna Menghadapi Berbagai
Ancaman Pertahanan Negara

No	Nama Lengkap	Tanda Tangan	Tanggal
1	Promotor: Prof. Dr. Marsetio, S.Sos., M.M., Laksamana TNI (Purn)		
2	Co-Promotor I: Kolonel Sus Dr. Ir. Rudy AG Gultom, MSc.		
3	Co-Promotor II: Brigjen TNI Dr. Pujo Widodo, S.E., M.A., MDS, M.Si., M.Si. (Han)		
4	Penguji Internal I: Mayjen TNI Dr. Joni Widjayanto, S.Sos., M.M., CIQnR, CIQaR		
5	Penguji Internal II: Prof. Dr. S. Pantja Djati, S.E., M.Si., M.A.		
6	Penguji Internal III: Dr. Siswo Hadi S., S.T., M.MT, CIRnR, CIQaR, Laksda TNI (Purn)		
7	Penguji Internal IV: Mayjen TNI Dr. Budi Pramono, S.I.P, M.M., M.A., (GSC), CIQaR, CIQnR		
8	Penguji Eksternal I: Prof. Dr. Ing. Kalamullah Ramli, M.Eng.		
9	Penguji Eksternal II: Prof. Dr. Ir. Eko Kuswardono Budiardjo, M.Sc.		

PERNYATAAN ORISINALITAS

Dengan ini saya menyatakan bahwa dalam tesis/disertasi ini tidak terdapat karya atau bagian karya yang pernah diajukan untuk memperoleh gelar kesarjanaan jenjang apapun di suatu Perguruan Tinggi; dan sepanjang sepengetahuan saya juga tidak terdapat istilah, frasa, kalimat, paragraph, subbab, atau bab dari karya yang pernah ditulis atau diterbitkan; kecuali yang secara tertulis diajukan dalam naskah ini dan disebutkan dalam Daftar Referensi serta Daftar Publikasi (*proceeding* dan jurnal yang telah dipublikasikan sebagai bagian tak terpisahkan dari persyaratan menyelesaikan disertasi dan Program Doktor).

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

Sentul, 11 Oktober 2021

Richardus Eko Indrajit

KATA PENGANTAR

Segala puji dan syukur peneliti panjatkan kehadirat Tuhan Yang Maha Kuasa karena berkat rahmat karunia-Nya maka penyusunan Disertasi Doktoral berjudul “Strategi Pengembangan Kebijakan Kedaulatan Pertahanan Siber Nasional Guna Menghadapi Berbagai Ancaman Pertahanan Negara” dapat diselesaikan dengan baik. Penyusunan Disertasi ini merupakan salah satu syarat dalam memperoleh gelar Doktor Ilmu Pertahanan pada Program Studi Ilmu Pertahanan, Fakultas Strategi Pertahanan. Universitas Pertahanan Indonesia.

Peneliti melalui kesempatan ini ingin menghaturkan ucapan terima kasih yang sebesar-besarnya kepada pihak-pihak yang secara langsung maupun tidak langsung telah berperan dalam penyusunan Disertasi ini. Secara khusus perkenankanlah peneliti mengucapkan terima kasih kepada segenap civitas akademika Universitas Pertahanan dan sejumlah pihak terkait lainnya, terutama:

1. Laksamana Madya TNI Prof. Dr. Amarulla Octavian, S.T., M.Sc., DESD., CIQnR., CIQaR., IPU selaku Rektor Universitas Pertahanan;
2. Mayjen TNI Dr. Joni Widjayanto, S.Sos., M.M., CIQnR, CIQaR selaku Plh Direktur Program Pasca Sarjana dan Penguji Internal I;
3. Prof. Dr. Marsetio, S.Sos., M.M., Laksamana TNI (Purn) selaku Promotor;
4. Kolonel Sus Dr. Ir. Rudy AG Gultom, MSc. Selaku Co-Promotor I;
5. Brigjen TNI Dr. Pujo Widodo, S.E., M.A., MDS, M.Si., M.Si. (Han) selaku Co-Promotor II;
6. Prof. Dr. S. Pantja Djati, S.E., M.Si., M.A. selaku Penguji Internal II;
7. Dr. Siswo Hadi S., S.T., M.MT, CIRnR, CIQaR, Laksda TNI (Purn) selaku Penguji Internal III;
8. Mayjen TNI Dr. Budi Pramono, S.I.P, M.M., M.A., (GSC), CIQaR, CIQnR selaku Penguji Internal IV;

9. Brigjen TNI Dr. Drs. Luhut Simbolon, M.Si., M.M. selaku Penguji Internal V;
10. Prof. Dr. Ing. Kalamullah Ramli, M.Eng. selaku Penguji Eksternal I;
11. Prof. Dr. Ir. Eko Kuswardono Budiardjo, M.Sc. selaku Penguji Eksternal II;
12. Seluruh guru besar, dosen, dan peneliti yang telah membagikan ilmunya selama proses pembelajaran berlangsung;
13. Segenap staf dan karyawan Program Studi Doktoral Universitas Pertahanan yang senantiasa memberikan dukungan serta layanan administratif selama proses pembelajaran dan penelitian berlangsung; dan
14. Rekan-rekan Mahasiswa Cohort-2 Program Studi Doktoral Universitas Pertahanan yang selalu kompak saling berbagi, bekerjasama, dan belajar secara kolektif dalam mencari ilmu serta tak pernah lelah memberikan masukan serta saran kepada peneliti.

Secara khusus tak lupa pula peneliti sampaikan ucapan terima kasih dan rasa cinta yang tulus kepada istri tercinta, Lisa A. Riyanto, serta anak-anak tercinta Satria, Tiara, Trisha, dan Theana, yang senantiasa sabar memberikan dukungan tak berkesudahan selama peneliti menuntut ilmu di Universitas Pertahanan. Terima kasih tak terhingga pula untuk kedua orang tua yang tak pernah lelah berdoa demi keberhasilan, kesehatan, dan kesuksesan peneliti dalam menekuni studi lanjutnya, demi memberikan sumbangan pemikiran bagi bangsa dan negara.

Akhir kata, peneliti sangat berharap agar karya Disertasi yang masih jauh dari sempurna ini dapat memberikan kontribusi yang signifikan bagi dunia pengetahuan dan Negara Kesatuan Republik Indonesia.

Sentul, 11 Oktober 2021

Richardus Eko Indrajit

ABSTRAK

**STRATEGI PENGEMBANGAN KEBIJAKAN KEDAULATAN
PERTAHANAN SIBER NASIONAL GUNA MENGHADAPI
BERBAGAI ANCAMAN PERTAHANAN NEGARA**

Richardus Eko Indrajit

Dinamika dunia pasca globalisasi telah mengubah lingkungan strategis berbagai negara di dunia. Berkembang pesatnya teknologi informasi dan komunikasi telah mengubah tatanan relasi dan kehidupan bernegara. Di satu sisi kehadiran teknologi informasi dan ruang siber memberikan manfaat bagi manusia. Pada sisi yang lain sejumlah ancaman baru mengemuka dalam rupa meningkatnya frekuensi dan volume serangan siber dalam satu negara atau antar negara. Berkaca pada serangan siber di masa lalu, dapat diambil kesimpulan bahwa keberadaannya dapat membahayakan kedaulatan bangsa, keutuhan negara, dan keamanan masyarakat. Untuk dapat menghadapi fenomena ini, Indonesia perlu menyusun dan mengembangkan strategi pengembangan kebijakan kedaulatan pertahanan siber nasional yang efektif, efisien, dan terkendali. Pengembangan strategi harus dilakukan dengan melihat permasalahan secara holistik, komprehensif, dan berbasis sistem. Tujuan penelitian ini adalah mengembangkan model strategi kebijakan penyusunan kebijakan kedaulatan siber nasional. Metodologi yang dipergunakan adalah *mixed-method* yang bertumpu pada metoda kualitatif yang diperkuat dengan dukungan data kuantitatif. *Baseline* metodologi yang dipergunakan adalah *Soft System Methodology*, yang dilengkapi dengan sejumlah metoda lain seperti: *Analytic Hierarchy Process (AHP)*, *rich picture*, *PESTEL*, *CATWOE*, *threat intelligence*, *cause-and-effect network*, *big data analysis*, analisis kebijakan, dan *risk assessment matrix*. Data primer dan sekunder diperoleh melalui sejumlah aktivitas, seperti wawancara, observasi, *forum group discussion*, *round table discussion*, studi pustaka, *benchmarking*, *traffic log files*, dan survei. Hasil penelitian memperlihatkan sejumlah temuan, yaitu: (i) taksonomi ancaman serangan siber ke wilayah NKRI; (ii) dampak strategis serangan siber terhadap pertahanan negara; (iii) tingkat kerawanan pertahanan siber nasional; (iv) efektivitas kebijakan pertahanan siber yang dimiliki Indonesia saat ini; (v) model

kebijakan kedaulatan pertahanan siber yang ideal; dan (vii) model strategi penyusunan dan pengembangan kebijakan kedaulatan pertahanan siber nasional.

Kata kunci: ancaman, kebijakan, pertahanan siber, strategi

ABSTRACT

STRATEGY FOR DEVELOPING A NATIONAL CYBER DEFENSE SOVEREIGNTY POLICY IN DEALING WITH VARIOUS STATE DEFENSE THREATS

Richardus Eko Indrajit

The dynamics of the world after globalization has changed the strategic environment of various countries in the world. The rapid development of information and communication technology has changed the order of relations and state life. On the one hand, the presence of information technology and cyberspace provides benefits for humans. On the other hand, a number of new threats have emerged in the form of increasing frequency and volume of cyber attacks within one country or between countries. Reflecting on past cyber attacks, it can be concluded that its existence can endanger the nation's sovereignty, state integrity, and public security. To be able to deal with this phenomenon, Indonesia needs to formulate and develop a strategy for developing a national cyber defense sovereignty policy that is effective, efficient, and controlled. Strategy development must be done by looking at the problem holistically, comprehensively, and system-based. The purpose of this study is to develop a strategic model for formulating national cyber sovereignty policies. The methodology used is a mixed-method which relies on qualitative methods which are supported by quantitative data. The baseline methodology used is the Soft System Methodology, which is complemented by a number of other methods such as: Analytic Hierarchy Process (AHP), rich picture, PESTEL, CATWOE, threat intelligence, cause-and-effect network, big data analysis, policy analysis, and risk assessment matrix. Primary and secondary data were obtained through a number of activities, such as interviews, observations, group discussion forums, round table discussions, literature studies, benchmarking, traffic log files, and surveys. The results of the study show a number of findings, namely: (i) taxonomy of cyber attack threats to the territory of the Republic of Indonesia; (ii) the strategic impact of cyber attacks on national defense; (iii) the level of vulnerability of the national cyber defense; (iv) the effectiveness of Indonesia's current cyber defense policy; (v) an ideal cyber defense sovereignty policy model; and (vii) a strategy model for formulating and developing a national cyber defense sovereignty policy.

Keywords: threat, policy, cyber defense, strategy

DAFTAR ISI

LEMBAR PERSETUJUAN UJIAN TERTUTUP.....	ii
LEMBAR PENGESAHAN DISERTASI.....	iv
PERNYATAAN ORISINALITAS.....	vi
KATA PENGANTAR.....	viii
ABSTRAK.....	x
<i>ABSTRACT</i>	xii
DAFTAR ISI.....	xiv
DAFTAR GAMBAR.....	xix

BAB 1 PENDAHULUAN 29

1.1 Latar Belakang	29
1.2 Fokus dan Sub Fokus	37
1.3 Rumusan Masalah	38
1.4 Tujuan Penelitian	40
1.5 Manfaat Penelitian	42
1.5.1 Manfaat Teoritis	42
1.5.2 Manfaat Praktis	43

BAB 2 TINJAUAN PUSTAKA 44

2.1 Landasan Teori	44
2.1.1 Filsafat Ilmu Pertahanan	44
2.1.2 Pertahanan dalam Konteks Keamanan Nasional	50
2.1.3 Pendekatan Kesisteman Sektor Pertahanan	55
2.1.4 Strategi dan Pengembangan Kebijakan	60

2.1.5	Perang dalam Doktrin Pertahanan Negara	62
2.1.6	Ancaman Teknologi Informasi dan Komunikasi	71
2.1.7	Karakteristik Dunia Siber	76
2.1.8	Kerawanan Siber dan Pertahanan Negara	77
2.1.9	Aktivitas Militerisasi dalam Dunia Siber	80
2.1.10	Penyusunan dan Pengembangan Kebijakan Publik	83
2.1.11	Soft System Methodology	90
2.1.12	Analytic Hierarchy Process	93
2.1.13	Risk Assesment Method	95
2.1.14	Cause-Effect Bayesian Network	96
2.2	Penelitian Terdahulu	97
2.3	Kerangka Pemikiran	119

BAB 3 METODOLOGI PENELITIAN 127

3.1	Metoda dan Desain Penelitian	127
3.2	Tempat dan Waktu Penelitian	136
3.3	Subyek dan Obyek serta Populasi dan Sampel Penelitian	137
3.4	Teknik Pengumpulan Data Kualitatif dan Kuantitatif	138
3.5	Teknik Pengolahan Data Kualitatif dan Kuantitatif	140
3.6	Teknik Analisis Data Kualitatif dan Kuantitatif	140

BAB 4 HASIL PENELITIAN DAN PEMBAHASAN 143

4.1	Deskripsi Data Terkait Obyek dan Subyek	151
4.2	Hasil Pengumpulan Data Kualitatif dan Kuantitatif	151

4.2.1	Potensi Ancaman Serangan Siber terhadap Pertahanan Negara	159
4.2.2	Dampak Serangan Siber terhadap Kedaulatan Negara	162
4.2.3	Tingkat Kerawanan Pertahanan Siber di Indonesia	163
4.2.4	Efektivitas Kebijakan Kedaulatan Pertahanan Siber di Indonesia	166
4.2.5	Model Pertahanan Siber Ideal yang Holistik dan Komprehensif	167
4.2.6	Strategi Pengembangan Kebijakan Pertahanan Siber Nasional	169
4.3	Hasil Pengolahan Data Kualitatif dan Kuantitatif	170
4.3.1	Potensi Ancaman Serangan Siber terhadap Pertahanan Negara	172
4.3.2	Dampak Serangan Siber terhadap Kedaulatan Negara	189
4.3.3	Tingkat Kerawanan Pertahanan Siber di Indonesia	222
4.3.4	Efektivitas Kebijakan Kedaulatan Pertahanan Siber di Indonesia	255
4.3.5	Model Pertahanan Siber Ideal yang Holistik dan Komprehensif	269
4.3.6	Strategi Pengembangan Kebijakan Pertahanan Siber Nasional	329
4.4	Hasil Analisis Kualitatif dan Kuantitatif	352
4.4.1	Potensi Ancaman Serangan Siber terhadap Pertahanan Negara	353
4.4.2	Dampak Serangan Siber terhadap Kedaulatan Negara	376
4.4.3	Tingkat Kerawanan Pertahanan Siber di Indonesia	397
4.4.4	Efektivitas Kebijakan Kedaulatan Pertahanan Siber di Indonesia	408
4.4.5	Model Pertahanan Siber Ideal yang Holistik dan Komprehensif	411
4.4.6	Strategi Pengembangan Kebijakan Pertahanan Siber Nasional	428
4.5	Interpretasi Data	441
4.5.1	Ancaman terhadap Kedaulatan Negara di Era Digital	443
4.5.2	Dampak Serangan Siber terhadap Kedaulatan Negara	446
4.5.3	Kerentanan dalam Ruang Siber Nasional	448
4.5.4	Kesiapan Regulasi dalam Konteks Pertahanan Siber	450

4.5.5	Ekosistem Ideal Pertahanan Siber Negara	452
4.5.6	Strategi Pengembangan Kebijakan Pertahanan Siber	454
4.6	Pembahasan	458
4.6.1	Indonesia dalam Pusaran Ancaman Serangan Siber	458
4.6.2	Dampak Serangan Siber terhadap Pertahanan NKRI	477
4.6.3	Kerentanan dan Kelemahan Sistem Pertahanan Siber Nasional	488
4.6.4	Efektivitas dan Kualitas Kebijakan Pertahanan Siber di Indonesia	496
4.6.5	Model Ekosistem Pertahanan Siber Ideal	509
4.6.5.1	Tujuan Negara Kesatuan Republik Indonesia	509
4.6.5.2	Ancaman Non-Militer dalam Ranah Siber	510
4.6.5.3	Lingkungan Strategis Dalam dan Luar Negeri	510
4.6.5.4	Pola Pikir dan Perilaku	511
4.6.5.5	Doktrin Pertahanan Siber	512
4.6.5.6	Kerangka Ekosistem Pertahanan Siber	512
4.6.5.7	Ekosistem Pertahanan Siber Nasional	516
4.6.5.8	Modus Dua Lingkungan Pertahanan Siber	516
4.6.5.9	Anatomi dan Struktur Kebijakan Siber	517
4.6.5.10	Politik dan Tata Kelola Siber Dunia	518
4.6.5.11	Interaksi dan Kolaborasi Stakeholder Siber	519
4.6.5.12	Ragam Komponen Pendukung Ekosistem	519
4.6.5.13	The Indonesia Cyber Terrain	524
4.6.6	Strategi Pengembangan Kebijakan Pertahanan Siber Nasional	530
4.6.6.1	UUD-RI dan Tujuan Negara	531
4.6.6.2	Doktrin Pertahanan Kedaulatan Siber Nasional	533
4.6.6.3	Domain Kebijakan Perlindungan Siber (Cyber Safeguarding)	534

4.6.6.4	Domain Kebijakan Pertahanan Siber (Cyber Defense)	536
4.6.6.5	Domain Kebijakan Penyerangan Siber (Cyber Offense)	539
4.6.6.6	Domain Kebijakan Peperangan Siber (Cyber Warfare)	541
4.6.6.7	Ragam Kebijakan Pendukung Tata Kelola Pertahanan Siber	544
4.6.6.8	Rangkaian Proses pada Empat Domain Siber	549
4.6.6.9	Pasukan Siber dan Kompetensinya	557
4.6.6.10	Kapabilitas dan Kemampuan	563
4.6.6.11	Prioritas Pengembangan Kebijakan Pertahanan Siber	565
4.6.6.12	Kebutuhan Pengembangan Kebijakan Pertahanan Siber	574
4.6.6.13	Pembagian Tugas dan Wewenang Tata Kelola Siber	584

BAB 5 KESIMPULAN DAN REKOMENDASI 590

5.1 Kesimpulan 590

5.2 Rekomendasi 594

5.2.1 Rekomendasi Teoritis 594

5.2.2 Rekomendasi Praktis 595

DAFTAR PUSTAKA..... 597

DAFTAR LAMPIRAN 630

DAFTAR GAMBAR

Gambar 2. 1 Perbedaan antara Berbagai Relasi Rumpun Keilmuan.....	50
Gambar 2. 2 Kerangka Sistem Sektor Pertahanan Negara	59
Gambar 2. 3 Matriks Tingkatan Keamanan Negara	68
Gambar 2. 4 Hubungan Dunia Fisik dan Siber dalam Militer	79
Gambar 2. 5 Faktor Ancaman terhadap Dunia Siber (Wardrop, 2015).....	80
Gambar 2. 6 Soft System Methodology.....	92
Gambar 2. 7 Analytic Hierarchy Process	94
Gambar 2. 8 Risk Assessment Matrix.....	96
Gambar 2. 9 Bayesian Network.....	97
Gambar 2. 10 Kerangka Berpikir Penelitian	119
Gambar 2. 11 Kerangka Prosedural Penelitian.....	122
Gambar 2. 12 Pertanyaan Penelitian dalam Kerangka Prosedural	124
Gambar 3. 1 <i>Soft System Methodology (SSM)</i>	129
Gambar 3. 2 Pemetaan SSM dan Pertanyaan Penelitian	130
Gambar 3. 3 Metoda Pendukung pada Setiap Tahap SSM	132
Gambar 4. 1 Rich Picture Kompleksitas Fenomena Pertahanan Siber.....	146
Gambar 4. 2 Klasterisasi terhadap Rich Picture	147
Gambar 4. 3 Sembilan Jenis Ancaman dan Serangan Siber pada Hanneg.....	176
Gambar 4. 4 Frekuensi Penyebutan Jenis Serangan pada 30 Literatur	188
Gambar 4. 5 Evolusi dan Kompleksitas Jenis Serangan Siber	207
Gambar 4. 6 Matrik Asesmen Risiko.....	213

Gambar 4. 7 Peta Komitmen Keamanan Siber Dunia menurut GSI	231
Gambar 4. 8 Skor Indonesia menurut ICT Development Index	234
Gambar 4. 9 Struktur Komponen Network Readiness Index	235
Gambar 4. 10 Skor Indonesia pada Sejumlah Komponen NRI.....	236
Gambar 4. 11 Grafik Kultur Mengelola Password.....	239
Gambar 4. 12 Grafik Kultur Mengunduh File dari Internet	240
Gambar 4. 13 Grafik Kultur Meminjamkan dan Dipinjami <i>Flash Disk</i>	241
Gambar 4. 14 Grafik Kultur Membackup File Penting	242
Gambar 4. 15 Grafik Kultur Menggunakan Kartu dan Uang Digital	243
Gambar 4. 16 Grafik Kultur Memindahkan Data antar Perangkat.....	244
Gambar 4. 17 Grafik Kultur Mengklik Tautan dan Membuka <i>Attachement</i>	246
Gambar 4. 18 Grafik Kultur Menggunakan Wifi Publik	247
Gambar 4. 19 Grafik Kultur Menggunakan Identitas Biometrik.....	248
Gambar 4. 20 Grafik Kultur Membaca dan Mengikuti Pelatihan	249
Gambar 4. 21 Grafik Kultur Menggunakan Situs E-Commerce	250
Gambar 4. 22 Grafik Kultur Menggunakan Aplikasi Virtual Meeting	251
Gambar 4. 23 Grafik Kultur Menggunakan Proprietary Software	252
Gambar 4. 24 Grafik Kultur Menggunakan Media Sosial dan Aplikasi Komunikasi	254
Gambar 4. 25 Grafik Pengalaman Mengalami Kasus Kejahatan Siber.....	255
Gambar 4. 26 Spektrum Kedaulatan Siber Amerika Serikat	275
Gambar 4. 27 Komitmen Nasional dan Politik Pertahanan Siber.....	276
Gambar 4. 28 Anatomi Doktrin Pertahanan Siber	277
Gambar 4. 29 Kerangka Konseptual Serangan Siber Nasional.....	277
Gambar 4. 30 Tingkatan Serangan Siber Negara.....	278
Gambar 4. 31 Anatomi Serangan Siber.....	280

Gambar 4. 32 Kerangka Konseptual Ruang Siber	282
Gambar 4. 33 Model Kapabilitas Pertahanan Siber.....	283
Gambar 4. 34 Klasifikasi Pertahanan Pasif Siber	284
Gambar 4. 35 Klasifikasi Pertahanan Aktif Siber	285
Gambar 4. 36 Klasifikasi Kolaborasi Pertahanan Siber	285
Gambar 4. 37 Klasifikasi Aktor Pertahanan Siber.....	286
Gambar 4. 38 Proses Pertahanan Siber secara End-to-End.....	289
Gambar 4. 39 Komponen Regulasi Pertahanan dan Keamanan Siber	295
Gambar 4. 40 Spektrum Pertahanan dan Keamanan Siber.....	298
Gambar 4. 41 Perbandingan Topologi Jaringan Kerjasama.....	299
Gambar 4. 42 Skenario Latihan Perang Siber	300
Gambar 4. 43 Model Kerjasama Saling Berbagi Sumber Daya	302
Gambar 4. 44 Karakteristik dan Indikator <i>Cyber Threat Intelligence</i>	304
Gambar 4. 45 Hirarki Regulasi terkait <i>Cyber Threat Intelligence</i>	304
Gambar 4. 46 Domain Pertahanan dan Keamanan Siber.....	305
Gambar 4. 47 Relasi Keterkaitan antar Proses Pertahan Siber	307
Gambar 4. 48 Domain Teritori Operasi Siber	309
Gambar 4. 49 Contoh Struktur Organisasi Siber dalam Kondisi Normal dan Krisis	310
Gambar 4. 50 Ragam Definisi Infrastruktur Kritis Nasional	312
Gambar 4. 51 Struktur Organisasi Penanganan Krisis Siber Amerika Serikat	313
Gambar 4. 52 Cyber Capability Defense Model.....	317
Gambar 4. 53 Kolaborasi Stakeholder Utama Pengelola Siber	320
Gambar 4. 54 Kerangka Filosofi Tata Kelola Siber di China	321
Gambar 4. 55 Ekosistem Strategis Tata Kelola Keamanan Siber	322
Gambar 4. 56 Tiga Lapisan Interkoneksi dalam Dunia Siber	323

Gambar 4. 57 Kerangka Heterogen Terdistribusi.....	325
Gambar 4. 58 Berbagi Peran dalam Pengelolaan Siber	327
Gambar 4. 59 Rich Picture Seputar Pertahanan Siber Nasional	343
Gambar 4. 60 Klasterisasi Rich Picture Seputar Pertahanan Siber Nasional	346
Gambar 4. 61 Domain Komponen Utama pada Ekosistem Pertahanan Siber Nasional.....	347
Gambar 4. 62 Relasi Keterkaitan antar Komponen pada Ekosistem Pertahanan Siber Nasional.....	348
Gambar 4. 63 Pemetaan CATWOE pada Ekosistem Pertahanan Siber Nasional	351
Gambar 4. 64 Dua Dunia dalam Kehidupan Manusia Moderen	365
Gambar 4. 65 Hubungan Keterkaitan antar Dua Dunia.....	366
Gambar 4. 66 Pengaruh Tak Terpisahkan antar Dua Dunia.....	367
Gambar 4. 67 Pengaruh Dunia Nyata terhadap Dunia Siber	369
Gambar 4. 68 Pengaruh Dunia Siber terhadap Dunia Nyata	372
Gambar 4. 69 Dampak Serangan <i>Identity Theft</i>	378
Gambar 4. 70 Dampak Serangan <i>Data Breach</i>	380
Gambar 4. 71 Dampak Serangan <i>Cyber-Espionage</i>	382
Gambar 4. 72 Dampak Serangan <i>Malware</i>	384
Gambar 4. 73 Dampak Serangan DDOS.....	387
Gambar 4. 74 Dampak Serangan <i>Insider Threat</i>	389
Gambar 4. 75 Dampak Serangan <i>Ransomware</i>	392
Gambar 4. 76 Dampak Serangan <i>Cryptojacking</i>	395
Gambar 4. 77 Tren Serangan dan Kejahatan Siber.....	397
Gambar 4. 78 Tiga Domain Keamanan Siber	399
Gambar 4. 79 Strategi Penanganan Domain Teknis.....	400
Gambar 4. 80 Strategi Penanganan Domain Bisnis	401
Gambar 4. 81 Strategi Penanganan Domain Sosial	403

Gambar 4. 82 Jejaring Keterkaitan antar Komponen Siber	406
Gambar 4. 83 Cyber Terrain (Riley, 2014) – US Department of Defense	423
Gambar 4. 84 Hubungan Keterkaitan antar Akar Masalah Pertahanan Siber.....	442
Gambar 4. 85 Profil Serangan terhadap Situs Militer Indonesia	463
Gambar 4. 86 Grafik 10 Anomali Trafik Selama Tahun 2020	464
Gambar 4. 87 Negara-Negara Sumber dan Destinasi Anomali Trafik Siber	466
Gambar 4. 88 Hasil Penetrasi Zone-H terhadap Situs Militer di Indonesia.....	480
Gambar 4. 89 Contoh Modus Serangan DDOS berupa Pemusatan ke Satu Destinasi	484
Gambar 4. 90 Cyber Exposure Index Indonesia.....	495
Gambar 4. 91 Regulasi sebagai Episentrum Ekosistem Pertahanan Siber.....	514
Gambar 4. 92 Kerangka Holistik Lingstra Pertahanan Siber Nasional.....	522
Gambar 4. 93 The Indonesia Cyber Terrain	525
Gambar 4. 94 Kerangka Kebijakan Pertahanan Siber Nasional	547
Gambar 4. 95 Profil dan Kapabilitas Pertahanan Siber Negara	548
Gambar 4. 96 Empat Dimensi Ruang Siber	550
Gambar 4. 97 Relasi pada Domain Kebijakan Perlindungan Siber	551
Gambar 4. 98 Relasi pada Domain Kebijakan Pertahanan Siber	552
Gambar 4. 99 Relasi pada Domain Kebijakan Penyerangan Siber	554
Gambar 4. 100 Relasi pada Domain Kebijakan Peperangan Siber.....	555
Gambar 4. 101 Relasi antar Komponen pada Domain Kebijakan Pendukung Tata kelola Pertahanan Siber.....	556
Gambar 4. 102 Struktur AHP.....	565

DAFTAR TABEL

Tabel 2. 1 Perbedaan Ilmu dan Pengetahuan	46
Tabel 2. 2 Perbandingan Karakteristik Perang Dingin dan.....	66
Tabel 2. 3 Tiga Layer Cyber Space.....	77
Tabel 2. 4 Faktor Ancaman terhadap Dunia Siber (Wardrop, 2015).....	81
Tabel 2. 5 Perbandingan Perang Konvensional dan Siber	82
Tabel 2. 6 Daftar Penelitian Relevan Terdahulu.....	100
Tabel 3. 1 Tata Kala Waktu Penelitian.....	136
Tabel 4. 1 Pemetaan Relasi Pertanyaan Penelitian terhadap Proses SSM.....	143
Tabel 4. 2 Pemetaan Model Pengumpulan Data terhadap Pertanyaan Penelitian..	152
Tabel 4. 3 Pemetaan Informan Penelitian	155
Tabel 4. 4 Metoda dan Hasil Pengumpulan Data Pertanyaan Penelitian Pertama..	160
Tabel 4. 5 Metoda dan Hasil Pengumpulan Data Pertanyaan Penelitian Kedua	162
Tabel 4. 6 Metoda dan Hasil Pengumpulan Data Pertanyaan Penelitian Ketiga	163
Tabel 4. 7 Metoda dan Hasil Pengumpulan Data Pertanyaan Penelitian Keempat..	166
Tabel 4. 8 Metoda dan Hasil Pengumpulan Data Pertanyaan Penelitian Kelima.....	168
Tabel 4. 9 Metoda dan Hasil Pengumpulan Data Pertanyaan Penelitian Keenam ..	169
Tabel 4. 10 Pemetaan Model Pengolahan Data terhadap Sumber Data	171
Tabel 4. 11 Hasil Pengolahan Data Potensi Ancaman Serangan Siber	172
Tabel 4. 12 Ragam Ancaman terhadap Sektor Pertahanan dan Dampaknya.....	177
Tabel 4. 13 Pemetaan Ragam Ancaman terhadap Literatur Ilmiah	180
Tabel 4. 14 Hasil Pengolahan Data Dampak Serangan Siber.....	189
Tabel 4. 15 Ancaman dan Tujuan Serangan Siber pada Sektor Pertahanan.....	191
Tabel 4. 16 Kasus Perang dan Serangan Siber antar Negara di Masa Lalu.....	193

Tabel 4. 17 Pemetaan Jenis Serangan terhadap Modus Serangan	212
Tabel 4. 18 Hasil Pemetaan Risiko Pakar Pertahanan Siber	215
Tabel 4. 19 Hasil Konversi Skor Asesmen Risiko	218
Tabel 4. 20 Prioritisasi Serangan	219
Tabel 4. 21 Hasil Pengolahan Data Tingkat Kerawanan Pertahanan Siber.....	222
Tabel 4. 22 Skor NCSI Indonesia terkait Indikator Umum	227
Tabel 4. 23 Skor NCSI Indonesia terkait Indikator Dasar.....	227
Tabel 4. 24 Skor NCSI Indonesia terkait Indikator Manajemen Krisis dan Insiden	229
Tabel 4. 25 Nilai Indonesia pada Sejumlah Pilar NRI	236
Tabel 4. 26 Nilai Indonesia pada Sejumlah Dimensi NRI.....	237
Tabel 4. 27 Hasil Pengolahan Data Efektivitas Kebijakan Pertahanan Siber	256
Tabel 4. 28 Daftar Peraturan dan Kebijakan Seputar Siber.....	258
Tabel 4. 29 Hasil Survei terkait Bahaya Serangan Siber terhadap Hanneg.....	265
Tabel 4. 30 Hasil Survei terkait Sumber Serangan Siber	265
Tabel 4. 31 Hasil Survei terkait Kedaulatan Siber	266
Tabel 4. 32 Hasil Survei terkait Potensi Kemampuan SDM Indonesia.....	267
Tabel 4. 33 Hasil Survei terkait Kebijakan Siber di Indonesia.....	267
Tabel 4. 34 Hasil Survei terkait Pimpinan pada Serangan Siber Masif.....	268
Tabel 4. 35 Hasil Survei terkait Strategi Pertahanan Siber.....	268
Tabel 4. 36 Hasil Pengolahan Data Model Pertahanan Siber Ideal.....	269
Tabel 4. 37 Tahapan Proses Serangan Siber	287
Tabel 4. 38 Ragam Model Pertahanan Siber	288
Tabel 4. 39 Bentangan Infrastruktur Telekomunikasi Indonesia	290
Tabel 4. 40 Sistem pada <i>Cyber Threat Intelligence</i>	293
Tabel 4. 41 Pembagian Peran Penanganan Ancaman Siber	300
Tabel 4. 42 Protokol <i>Cyber Intelligence</i>	302

Tabel 4. 43 Tipe Peretas, Motivasi, dan Keahliannya	307
Tabel 4. 44 Komponen Militerisasi di Dunia Siber	316
Tabel 4. 45 Ragam Aktivitas IGO.....	317
Tabel 4. 46 Ragam Aktivitas IITO	318
Tabel 4. 47 Ragam Aktivitas CSIRT/CERT	319
Tabel 4. 48 Hasil Pengolahan Data Strategi Pengembangan Kebijakan Pertahanan Siber Nasional.....	329
Tabel 4. 49 Triangulasi Hasil Penelitian terhadap Pertanyaan Pertama	376
Tabel 4. 50 Triangulasi Hasil Penelitian terhadap Pertanyaan Kedua.....	396
Tabel 4. 51 Triangulasi Hasil Penelitian terhadap Pertanyaan Ketiga.....	407
Tabel 4. 52 Triangulasi Hasil Penelitian terhadap Pertanyaan Keempat	411
Tabel 4. 53 Ancaman Serangan berbasis Lapisan Teknologi	424
Tabel 4. 54 Triangulasi Hasil Penelitian terhadap Pertanyaan Kelima	427
Tabel 4. 55 Gap pada Doktrin Pertahanan dan Kedaulatan Siber Negara	429
Tabel 4. 56 Gap pada Prinsip, Paradigma, dan Kerangka Kebijakan.....	430
Tabel 4. 57 Gap pada Ekosistem Pertahanan Siber Nasional.....	431
Tabel 4. 58 Gap pada Jaringan Infrastruktur Telekomunikasi dan Internet	433
Tabel 4. 59 Gap pada Suprastruktur Pertahanan Siber	435
Tabel 4. 60 Gap pada Sistem Peraturan dan Perundang-Undangan	435
Tabel 4. 61 Gap pada Struktur Kelembagaan dan otoritas Kolektif	436
Tabel 4. 62 Gap pada Industri Teknologi dan Informasi Nasional.....	437
Tabel 4. 63 Gap pada Kooperasi Nasional dan Internasional	438
Tabel 4. 64 Gap pada Standar Pertahanan dan Keamanan Siber	439
Tabel 4. 65 Gap pada Sumber Daya Manusia dan Pasukan Siber	440
Tabel 4. 66 Triangulasi Hasil Penelitian terhadap Pertanyaan Keenam	440
Tabel 4. 67 Pemetaan Akar Permasalahan ke dalam Konteks Pertanyaan Penelitian	442

Tabel 4. 68 Pemetaan Kapabilitas dan Kemampuan Pasukan Siber	563
Tabel 4. 69 Hasil Pengolahan Data AHP: Kriteria Utama.....	568
Tabel 4. 70 Hasil Pengolahan Data AHP: Ugensitas	568
Tabel 4. 71 Hasil Pengolahan Data AHP: Implementasi.....	570
Tabel 4. 72 Hasil Pengolahan Data AHP: Tantangan	571
Tabel 4. 73 Hasil Pengolahan Data AHP: Efektivitas.....	572
Tabel 4. 74 Hasil Pengolahan Data AHP: Manfaat.....	573
Tabel 4. 75 Daftar Usulan Amandemen UUD-RI.....	575
Tabel 4. 76 Daftar Usulan Ketetapan MPR.....	576
Tabel 4. 77 Daftar Usulan Undang-Undang	576
Tabel 4. 78 Daftar Usulan Peraturan Pemerintah.....	577
Tabel 4. 79 Daftar Usulan Keputusan Presiden	578
Tabel 4. 80 Daftar Usulan Peraturan (Bersama) Menteri.....	578
Tabel 4. 81 Pembagian Peran secara Kolektif	586

