

BAB IV

PENUTUP

17. Simpulan.

Pada Abad Ke-XXI ruang siber telah dimanfaatkan secara luas untuk mendukung penyelenggaraan tugas pemerintahan, militer, maupun kehidupan manusia modern dalam kehidupan sehari-hari. Namun, selain memberikan dampak positif terutama dalam hal kemudahan dalam berkomunikasi maupun berbagi informasi, pemanfaatan ruang siber tersebut juga memiliki kerawanan yang dapat berdampak negatif, salah satunya berupa serangan siber terhadap infrastruktur strategis nasional suatu negara. Serangan siber yang dapat berupa serangan virus komputer (*malware*), upaya peretasan (*hacking*) terhadap sistem keamanan, pencurian data yang disimpan secara digital, atau pengambil alihan kontrol atas sistem yang mengendalikan infrastruktur strategis nasional tersebut berpeluang untuk membahayakan kedaulatan negara, keutuhan wilayah NKRI, serta keselamatan segenap bangsa dan negara Indonesia. Dalam perspektif militer, pemanfaatan ruang siber sebagai ranah peperangan baru selain ranah perang darat, laut, udara dan ruang angkasa telah membuka peluang bagi musuh untuk dapat melumpuhkan sistem komando dan kendali, merusak jaringan komputer dan komunikasi, ataupun mengacaukan sistem elektronik Alutsista, dengan tujuan agar musuh mencapai kemenangan dalam peperangan. Selain itu, serangan siber terhadap infrastruktur strategis nasional diperkirakan dapat menghambat, menghalangi, maupun menggagalkan pelaksanakan tugas TNI khususnya TNI Angkatan Udara pada masa yang akan datang.

Melalui analisis permasalahan tentang peran TNI dalam mendukung pengamanan infrastruktur strategis nasional dan dengan didasarkan pada perkembangan lingkungan strategis khususnya yang berkaitan dengan ancaman siber serta data dan fakta tentang serangan siber yang pernah terjadi di Indonesia, maka dapat dirumuskan suatu kesimpulan sebagai berikut:

- a. TNI sebagai komponen utama pertahanan negara memerlukan regulasi yang dapat dijadikan dasar hukum sekaligus rujukan dalam penyelenggaraan pertahanan siber, khususnya yang mengatur peran dan mekanisme pelibatan TNI dalam menanggulangi serangan siber

terhadap infrastruktur strategis nasional. Dengan mempertimbangkan adanya kebutuhan akan suatu regulasi yang dapat dijadikan dasar hukum serta referensi dalam pelibatan TNI untuk menanggulangi ancaman siber, khususnya dalam konteks perang siber, maka peraturan perundang-undangan yang perlu direvisi antara lain adalah:

- 1) Undang-Undang RI Nomor 3 Tahun 2002 Tentang Pertahanan, yaitu dengan menambahkan “ancaman siber” di dalam Pasal 1 Undang-Undang Pertahanan yang memuat pengertian serta menjelaskan tentang ancaman siber yang dilakukan oleh negara maupun ancaman siber yang dilakukan oleh kelompok lain yang didukung oleh suatu negara, ancaman berupa serangan siber terhadap infrastruktur strategis nasional, atau ancaman berupa perang siber yang berpotensi membahayakan kedaulatan negara, keutuhan wilayah NKRI, serta keselamatan segenap bangsa Indonesia.
- 2) Undang-Undang RI Nomor 34 Tahun 2004 Tentang Tentara Nasional Indonesia (TNI), yaitu dengan menambahkan pengertian tentang ancaman non militer dan ancaman hibrida di dalam Pasal 1 Undang-Undang TNI, termasuk mencantumkan bentuk-bentuk ancaman hibrida yang memadukan ancaman konvensional dengan ancaman non konvensional seperti ancaman perang kimia, biologi, radiologi, nuklir, ancaman siber, serta mengklasifikasikan ancaman non konvensional tersebut sebagai bentuk ancaman militer.
- 3) Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber, yaitu dengan mencantumkan peran TNI sebagai alat negara dalam bidang pertahanan siber serta menambahkan ketentuan (pedoman) tentang penyelenggaraan sistem pertahanan siber nasional yang menempatkan TNI sebagai komponen utama dalam menghadapi perang siber.
- 4) Keputusan Panglima TNI Nomor Kep/1355/XII/2018 tentang Doktrin Siber TNI, yaitu dengan mencantumkan pembentukan organisasi Komando Siber TNI yang memiliki tugas, fungsi, dan kewenangan untuk merencanakan, melaksanakan, dan mengendalikan kegiatan dan operasi siber, baik yang bersifat defensif maupun yang bersifat ofensif, pada seluruh organisasi

- siber Angkatan Darat, Angkatan Laut, dan Angkatan Udara serta mengkoordinasikan kegiatan dan operasi siber pada seluruh Kementerian dan Lembaga Republik Indonesia sebagai sebuah sistem pertahanan siber nasional yang terintegrasi dalam rangka untuk menghadapi perang siber.
- b. Berdasarkan fakta bahwa saat ini ruang siber telah dimanfaatkan sebagai media peperangan baru, baik dalam konteks yang lebih luas untuk mencapai tujuan nasional suatu negara ataupun dalam konteks ancaman hibrida yang memadukan ancaman konvensional (serangan militer dan perang terbuka) dengan ancaman non konvensional (serangan siber dan perang siber), dapat dinyatakan bahwa Indonesia memerlukan organisasi pertahanan siber, sebagaimana bentuk Komando Siber (*Cyber Command*) yang dikembangkan oleh Angkatan Bersenjata Amerika Serikat (*U.S. Cyber Command*) atau Angkatan Bersenjata Singapura (*SAF Cyber Command*). Kesimpulan ini didapatkan berdasarkan fakta bahwa Pusat Pertahanan Siber (Pushansiber) yang ada di lingkungan Kementerian Pertahanan (Kemhan) saat ini tidak memiliki tugas, fungsi, dan kewenangan untuk merencanakan, melaksanakan, mengendalikan dan mengintegrasikan kegiatan dan operasi siber pada tataran nasional, baik yang bersifat defensif maupun ofensif, terutama karena Permenhan RI Nomor 82 Tahun 2014⁷³ dan Permenhan RI Nomor 2 Tahun 2017⁷⁴ hanya menyatakan bahwa tugas Pushansiber Kemhan adalah untuk mewujudkan ketahanan dan keamanan siber secara internal di dalam lingkungan Kemhan dan TNI.⁷⁵ Demikian juga yang terjadi pada lingkup Mabes TNI. Satuan Siber TNI juga tidak memiliki tugas, fungsi, dan kewenangan untuk merencanakan, melaksanakan, dan mengendalikan kegiatan dan operasi siber pada seluruh matra Angkatan Darat, Angkatan Laut, dan Angkatan Udara, khususnya dalam menghadapi ancaman berupa serangan siber terhadap infrastruktur strategis nasional ataupun perang siber.
 - c. Selain memerlukan organisasi pertahanan siber nasional, dapat disimpulkan pula bahwa kuantitas dan kualitas personel dalam bidang

⁷³ Peraturan Menteri Pertahanan RI Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber.

⁷⁴ Peraturan Menteri Pertahanan Nomor 2 Tahun 2017 tentang Organisasi dan Tata Kerja Kementerian Pertahanan.

⁷⁵ Op.Cit. halaman 20.

siber di lingkungan Kementerian Pertahanan dan TNI masih terbatas, sehingga untuk meningkatkan kemampuan siber TNI khususnya TNI Angkatan Udara diperlukan adanya peningkatan kemampuan SDM TNI dalam bidang siber. Dalam perspektif TNI, pemenuhan SDM siber ini dapat dilakukan dengan meningkatkan kemampuan prajurit TNI yang saat ini mengawaki organisasi siber di lingkungan Kementerian Pertahanan dan TNI, dengan menyelenggarakan program pendidikan, pelatihan, dan sertifikasi personel sesuai dengan standar kompetensi siber yang telah ditetapkan oleh Badan Siber dan Sandi Negara (BSSN). Selain meningkatkan kemampuan, dalam jangka panjang, pemenuhan pengawakan organisasi TNI dapat dilaksanakan melalui kerjasama antara TNI dengan Kementerian Pertahanan, Kementerian Komunikasi dan Informasi, Badan Siber dan Sandi Negara, Perusahaan Swasta Nasional, Organisasi Profesi, ataupun Lembaga Masyarakat yang bergerak dalam bidang siber sesuai dengan profesi, bidang tugas, dan kapasitas masing-masing, berdasarkan Undang-Undang RI Nomor 23 Tahun 2019 tentang Pengelolaan Sumber Daya Nasional Untuk Pertahanan Negara.

- d. Dalam prosesnya, pembuatan regulasi dalam bidang pertahanan siber, pengembangan organisasi siber, serta pemenuhan kebutuhan personel siber, keseluruhan upaya yang dilakukan untuk meningkatkan kemampuan siber TNI khususnya TNI Angkatan Udara memerlukan adanya pemenuhan dukungan sarana dan prasarana untuk menanggulangi ancaman berupa serangan siber dan perang siber. Meskipun sejak tahun 2018, Kemhan dan Mabes TNI telah berupaya untuk melengkapi sarana dan prasarana yang diperlukan oleh organisasi siber di lingkungan Kemhan dan TNI, namun masih terkendala oleh beberapa faktor, antara lain ketersediaan anggaran dan prioritas penggunaan anggaran pertahanan negara.
- 18. Rekomendasi.** Untuk mewujudkan peningkatan kemampuan siber TNI Angkatan Udara agar mampu menanggulangi serangan siber dalam rangka mendukung pengamanan infrastruktur strategis nasional, direkomendasikan saran sebagai berikut:
- a. Presiden bersama dengan DPR RI direkomendasikan untuk menyusun Rancangan Undang-Undang Pertahanan dan Keamanan Siber yang

dapat dipergunakan sebagai dasar hukum sekaligus rujukan dalam penyelenggaraan pertahanan siber, dengan mencantumkan peran dan mekanisme pelibatan TNI dalam menanggulangi serangan siber yang membahayakan bangsa dan negara Indonesia. Selain itu, Presiden bersama dengan DPR RI juga merevisi peraturan perundang-undangan Republik Indonesia dalam bidang pertahanan negara untuk diselaraskan dengan Undang-Undang Pertahanan dan Keamanan Siber.

- b. Menteri Pertahanan RI merevisi Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber, dengan mencantumkan peran TNI sebagai alat negara dalam bidang pertahanan siber serta menambahkan ketentuan tentang penyelenggaraan sistem pertahanan siber nasional yang menempatkan TNI sebagai Komponen Utama, Kementerian/Lembaga terkait sebagai Komponen Cadangan, dan potensi sumber daya nasional dalam bidang siber sebagai Komponen Pendukung, serta membuat Nota Kesepahaman antara Kementerian Pertahanan dengan Kementerian/Lembaga terkait untuk mengintegrasikan seluruh komponen pertahanan siber dalam suatu sistem pertahanan siber nasional.
- c. Panglima TNI merevisi Keputusan Panglima TNI Nomor Kep/1355/XII/2018 tentang Doktrin Siber TNI, dengan mencantumkan klausul yang menyatakan bahwa Satuan Siber TNI memiliki tugas, fungsi, dan kewenangan untuk merencanakan, melaksanakan, dan mengendalikan kegiatan dan operasi siber, baik yang bersifat defensif maupun yang bersifat ofensif, pada seluruh satuan siber pada Mabes Angkatan, serta membuat Perjanjian Kerjasama dengan Kementerian serta Lembaga negara terkait untuk mengkoordinasikan kegiatan dan operasi siber guna menghadapi ancaman siber pada masa damai ataupun pada masa perang.
- d. Kepala Staf Angkatan Udara (Kasau) merevisi Peraturan Kasau Nomor 19 Tahun 2020 Tanggal 8 Juni 2020 Tentang Organisasi dan Tugas Organisasi Dinas Pengamanan dan Persandian TNI Angkatan Udara (Dispamsanau), yang merupakan dasar pembentukan Satuan Siber sebagai salah satu Satuan Kerja (Satker) di bawah Dispamsanau, dengan menetapkan Peraturan Kasau yang baru tentang pembentukan Satuan Siber TNI Angkatan Udara sebagai Badan Pelaksana Pusat

(Balakpus) pada tingkat Mabesau di bawah supervisi Asisten Intelijen Kasau.

- e. Kementerian Pertahanan membuat Nota Kesepahaman dan Mabes TNI menindaklanjuti dengan membuat Perjanjian Kerjasama dengan Kementerian/Lembaga negara terkait, dalam rangka untuk memenuhi kebutuhan kuantitas dan kualitas personel TNI serta sarana dan prasarana organisasi siber di lingkungan Kementerian Pertahanan dan TNI yang diperlukan dalam penanggulangan ancaman siber terhadap infrastruktur strategis nasional.
- f. DPR RI dan Presiden perlu membuat rancangan undang-undang tentang Keamanan Nasional yang diharapkan dapat memperkuat dan memperjelas tugas, peran dan fungsi masing-masing Kementerian/Lembaga dalam kerangka menjaga kepentingan nasional dan melindungi warga negara Indonesia terhadap berbagai bentuk ancaman dan gangguan yang datang baik dari dalam dan luar negeri secara terpadu dan terintegrasi.

Jakarta, 25 Agustus 2021

Peserta,



Donald Kasenda, S.T., S.I.P., M.M.

Marsekal Pertama TNI

Lampiran:

- 1. Alur Pikir.
- 2. Riwayat Hidup.

DAFTAR PUSTAKA

Buku Referensi

- Amos Jordan, William Taylor, dan Michael Mazarr.1999. *American National Security*, Baltimore: Johns Hopkins University Press.
- Christopher Whyte dan Brian Mazanec. 2019. *Understanding Cyber Warfare: Politics, Policy and Strategy*, New York : Routledge.,
- Fabio Rugge (Ed.). 2018. *Confronting an “Axis of Cyber”? China, Iran, North Korea, Russia in Cyberspace*, ISPI (Italian Institute for International Political Studies), Milan: LediPublishing.
- George R. Terry dan Leslie W. Rue. 2012. *Dasar-Dasar Manajemen*, Cetakan Ke-13, Jakarta: Bumi Aksara.
- Hermawan Sulistyo (Ed.). 2012. *Dimensi-Dimensi Kritis Keamanan Nasional*, Jakarta : Pensil-324,
- James A. Green (Ed.). 2015. *Cyber Warfare: A Multidisciplinary Analysis*, New York: Routledge.
- Jason Andress and Steve Winterfeld. 2014. *Cyber Warfare: Techniques, Tactics And Tools For Security Practitioners*, Second Edition, Waltham: Syngress-Elsevier Inc.
- Jeffrey Carr. 2011. *Inside Cyber Warfare*, Second Edition, California: O'Reilly Media, Inc.
- Joseph Migga Kizza. 2014. *Computer Network Security and Cyber Ethics*, Jefferson, North Carolina: McFarland & Company, Inc.
- Mohan B. Gazula.2017. *Cyber Warfare Conflict Analysis and Case Studies*, Cybersecurity Interdisciplinary Systems Laboratory (CISL), Massachusetts Institute of Technology (MIT).
- Paschal Preston. 2001. *Reshaping Communications: Technology, Information and Social Change*, London: SAGE Publications Ltd.

Pusat Bahasa Departemen Pendidikan Nasional. 2008. *Kamus Besar Bahasa Indonesia (KBBI)*, Jakarta.

Quentin E. Hodgson, et.al. 2019. *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace*, Santa Monica: RAND Corporation.

Raphael S. Cohen, et.al. 2020. *The Future of Warfare in 2030: Project Overview and Conclusions*, Santa Monica: RAND Corporation.

Richard A. Clarke dan Robert K. Knake. 2010. *Cyber War: The Next Threat To National Security And What To Do About It*, New York: Harper Collins.

Sayidiman Suryohadiprojo. 2010. *Si Vis Pacem Para Bellum: Membangun Pertahanan Negara Yang Modern Dan Efektif*, Edisi Revisi, Jakarta: Pustaka Intermasa.

T. Hari Prihartono (Koord.). 2006. *Keamanan Nasional: Kebutuhan Membangun Perspektif Integratif Versus Pembiaran Politik dan Kebijakan*, Jakarta : Propatria Institute.

Thomas C. Reed. 2004. *At the Abyss: An Insider's History of the Cold War*, New York: Ballantine Books.

Winardi. 1999. *Pengantar Manajemen Penjualan*, Bandung: PT. Citra Aditya Bakti.

W.J.S. Poewadarminta.1986. *Kamus Besar Umum Indonesia*, Jakarta: Balai Pustaka.

Jurnal Dan Tesis

Bambang Tri Sutrisno. Juni 2016. *Urgensi Komando Pertahanan Siber (Cyber Defense Command) Dalam Menghadapi Perang Asimetris*, Lembaga Kajian Pertahanan Untuk Kedaulatan NKRI “Keris”, Jurnal Defendonesia, Volume 1 Nomor 2.

Denik Iswardani Witarti. 2011. *Tinjauan Teoritis Mengenai Konsep Keamanan Nasional*, dalam Jurnal Transnasional Volume 6 Nomor 1 Juni 2011, Jurusan Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Budi Luhur.

Jajang Rismanto, Suhirwan, dan Haposan Simatupang. 2020. *Implementasi Sistem Komunikasi Dalam Tugas Pokok TNI AU*, Program Studi Strategi Pertahanan Darat Fakultas Strategi Pertahanan, Jurnal Strategi Pertahanan Darat, Volume 6 Nomor 1.

Jonathan W. Sims. 2011. *Cybersecurity: The Next Threat to National Security*, Thesis Master of Military Studies, USMC Command and Staff College, Quantico: Marine Corps University.

Kenneth Geers. 2009. *The Cyber Threat to National Critical Infrastructures: Beyond Theory*, Information Security Journal: A Global Perspective, Volume 18, Issue 1.

Lawrence J. Trautman dan Peter C. Ormerod,. January 2018. *Wannacry, Ransomware, And The Emerging Threat To Corporations*, Social Science Research Network (SSRN), SSRN Electronic Journal.

Mariusz Antoni Kamiński. 6 Juni 2020. *Operation “Olympic Games”: Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran’s nuclear programme*, Faculty of National Security, War Studies University, Warsaw, Poland, Security and Defence Quarterly.

Omry Haizler, January 2017. *The United States’ Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking*, Cyber, Intelligence, and Security Journal, Volume 1 Nomor 1.

Patrick D. Allen, Col. dan Chris Demchak, Lt.Col. (US Army). March-April 2003. *The Palestinian and Israeli Cyberwar*, The Military Review.

Sidratahta Mukhtar. November 2011. *Keamanan Nasional: Antara Teori dan Prakteknya di Indonesia*, Jurnal Sociae Polities, Edisi Khusus.

Qian Chen dan Robert A. Bridges. 2017. *Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware*, The Institute of Electrical and Electronics Engineers (IEEE).

Untung Basuki, et.al. September 2018. *Optimalisasi Kemampuan Dan Akselerasi Implementasi Pembangunan Dan Pengembangan Sistem Informasi TNI AU Guna Mewujudkan Informasi Yang Akurat Dalam Rangka Mendukung Tugas TNI AU*, Staf Ahli Markas Besar TNI Angkatan Udara.

Peraturan Perundang-Undangan

Undang-Undang Republik Indonesia Nomor 3 Tahun 2002 Tentang Pertahanan Negara.

Undang-Undang Republik Indonesia Nomor 34 Tahun 2004 Tentang Tentara Nasional Indonesia (TNI).

Peraturan Presiden RI Nomor 58 Tahun 2015 Tentang Kementerian Pertahanan.

Peraturan Presiden RI Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN).

Peraturan Presiden RI Nomor 62 Tahun 2016 Tentang Perubahan Susunan Organisasi Tentara Nasional Indonesia (TNI).

Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber.

Peraturan Menteri Pertahanan Republik Indonesia Nomor 23 Tahun 2015 Tanggal 20 November 2015 Tentang Buku Putih Pertahanan.

Keputusan Panglima TNI Nomor Kep/555/VI/2018 Tentang Doktrin TNI Tri Dharma Eka Karma.

Keputusan Panglima TNI Nomor Kep/545/V/2019 tentang Doktrin TNI AU Swa Bhuwana Paksa.

Keputusan Panglima TNI Nomor Kep/1355/XII/2018 Tentang Doktrin Siber TNI.

Peraturan Panglima TNI Nomor 71 Tahun 2019 tanggal 31 Desember 2019 tentang Organisasi Dan Tugas Satuan Siber Tentara Nasional Indonesia (Satsiber TNI).

Naskah Akademik Rancangan Undang-Undang Keamanan dan Ketahanan Siber.

Naskah Akademik Rancangan Peraturan Badan Siber dan Sandi Nasional (BSSN) tentang Perlindungan Infrastruktur Informasi Kritis Nasional.

Internet

Adam Rizal, “*Ini Alasan Serangan Siber di Indonesia Melonjak Tajam Tahun ini*”, Info Komputer, 13 Oktober 2020,
[<https://infokomputer.grid.id/read/122379462/ini-alasan-serangan-siber-di-indonesia-melonjak-tajam-tahun-ini>].

Encyclopaedia Britannica, [<https://www.britannica.com>].

Agustinus Mario Damar, “*Indonesia Alami 205 Juta Serangan Siber Sepanjang 2017*”, Liputan 6, 22 Desember 2018,
[<https://www.liputan6.com/tekno/read/3203987/indonesia-alami-205-juta-serangan-siber-sepanjang-2017>].

AirNav Indonesia, “*Perkuat Sinergi Jaga Kedaulatan Ruang Udara, AirNav-TNI AU Tanda Tangani Perjanjian Kerja Sama*”, 26 April 2019,
[<https://www.airnavindonesia.co.id/perkuat/sinergi/jaga/kedaulatan/ruang/udara/airnav-tni/au/tanda/tangani/perjanjian/kerja/sama>].

Ajinkya Bagade, “*Singapore Announces Cyber Command To Defend On The Cyberspace Frontier*”, Information Security Report, 3 Maret 2020,
[<https://informationsecurity.report/news/cyberthreats-the-new-threat-frontier-for-singapore-armed-forces/7156>].

Antara, “*Pengoperasian Pusat Operasi Keamanan Siber Nasional akhir Desember*”, 4 Desember 2019,
[<https://www.antaranews.com/berita/1193579/pengoperasian-pusat-operasi-keamanan-siber-nasional-akhir-desember>].

Asian Development Bank (ADB), “*Laporan ADB: Pertumbuhan Ekonomi Negara-Negara Berkembang Di Asia Akan Menurun Tetapi Stabil*”, 11 April 2012,
[<https://www.adb.org/id/news/developing-asia-growth-subdued-steady-adb-report>].

Badan Siber dan Sandi Nasional (BSSN), “*Strategi Keamanan Siber Nasional*”, 2018, [<https://bssn.go.id/strategi-keamanan-siber-nasional>].

Badan Siber dan Sandi Nasional (BSSN), *Rancangan Peraturan Badan Siber dan Sandi Nasional (BSSN) tentang Perlindungan Infrastruktur Informasi Kritis Nasional*, [<https://bssn.go.id/sosialisasi-dan-permintaan-tanggapan-atas->

rancangan-peraturan-bssn-tentang-perlindungan-infrastruktur-informasi-kritis-nasional-iikn].

Berita Satu, “*BSSN Berharap RUU Keamanan dan Ketahanan Siber Segera Disahkan*”, [<https://www.beritasatu.com/nasional/569165/bssn-berharap-ruu-keamanan-dan-ketahanan-siber-segera-disahkan>].

Center for Strategic and International Studies (CSIS), “*Significant Cyber Incidents*”, [<https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>].

CNN, “*China-U.S. Cyber War Escalates*”, 1 Mei 2001,
 [<https://edition.cnn.com/2001/WORLD/asiapcf/east/04/27/china.hackers/index.html>]

Cyber Security Agency of Singapore (CSA), [<https://www.csa.gov.sg>].

CSA, “*Deputy Prime Minister Heng Swee Keat launches Singapore’s Safer Cyberspace Masterplan 2020*”, 6 Oktober 2020,
 [<https://www.csa.gov.sg/news/press-releases/safer-cyberspace-masterplan-launch>].

Dewan Teknologi Informasi dan Komunikasi Nasional (Wantiknas),
Pengembangan Keamanan Siber Nasional, November 2018,
 [<http://www.wantiknas.go.id/wantiknas-storage/file/img/kajian>

Dhiraphol Suwanprateep, “*Thailand Cybersecurity Act is Effective*”, Baker-Mckenzie, 28 Mei 2019,
 [<https://www.bakermckenzie.com/en/insight/publications/2019/05/thailand-cybersecurity-act-is-effective>].

Dispenau, “*TNI AU Kerjasama Dengan BMKG*”, 13 Januari 2015, [<https://tni-au.mil.id/tni-au-kerjasama-dengan-bmkg>].

DPR RI, *Naskah Akademik Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber*, 17 Juni 2019, [<http://dpr.go.id/doksileg/proses1/RJ1-20190617-025848-5506.pdf>]

Government Communications Headquarters (GCHQ), “*Director's speech at Cyber UK 2018*”, 22 Maret 2019, [<https://www.gchq.gov.uk/speech/director-cyber-uk-speech-2018>].

Gus W. Weiss, “*The Farewell Dossier: Duping The Soviets, Studies in Intelligence*”, Central Intelligence Agency, 1996, [<https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol39no5/pdf/v39i5a14p.pdf>].

ID-SIRTII/CC, *Laporan Tahunan Periode Januari-Desember 2018*, [<https://idsirtii.or.id/halaman/tentang/laporan-kegiatan.html>].

Iwan Sumantri, *Tren Serangan Siber Nasional 2016 Dan Prediksi 2017*, National Cyber Security Defence (NCSD), 4 Maret 2017, [<https://owasp.org/images/4/47/Iwan-OWASP-Cyber-Security-Trends-2017.pdf>]

Jeremy Wagstaff, “*Vietnam's Neighbors, Asean, Targeted by Hackers: Report*”, Jakarta Globe, 8 November 2017, [<https://jakartaglobe.id/news/vietnams-neighbors-asean-targeted-hackers-report>].

John P. Formichella, Artima Brikshasri, dan Naytiwut Jamallsawat, “*Cybersecurity Law In Thailand*”, Mondaq, 2 Desember 2019, [<https://www.mondaq.com/security/870568/cybersecurity-law-in-thailand>].

Kate Fazzini, “*In India-Pakistan conflict, there's a long-simmering online war, and some very good hackers on both sides*”, CNBC, 27 Februari 2019, [<https://www.cnbc.com/2019/02/27/india-pakistan-online-war-includes-hacks-social-media.html>].

Kementerian Komunikasi dan Informatika RI, “*Konferensi Pers Penanganan Penyebaran Virus WannaCry*”, 14 Mei 2017, [<https://www.kominfo.go.id/content/detail/9925/konferensi-pers-penanganan-penyebaran-virus-wannacry-14052017/0>].

Kementerian Perhubungan RI, “*Kemenhub Sambut Baik Kerjasama AP II dan TNI AU*”, 31 Januari 2011, [<http://dephub.go.id/post/read/kemenhub-sambut-baik-kerjasama-ap-ii-dan-tni-au-3186>].

Kevin Townsend, “*U.S. Cyber Command Launched DDoS Attack Against North Korea: Report*”, Security Week, 2 Oktober 2017,

[<https://www.securityweek.com/us-cyber-command-launched-ddos-attack-against-north-korea-report>].

Kompas, “RUU Siber Disebut Untuk Tegaskan Kewenangan BSSN”, 23 Agustus 2019, [<https://nasional.kompas.com/read/2019/08/23/19283341/ruu-siber-disebut-untuk-tegaskan-kewenangan-bssn>].

Lely Maulida, “205 Juta Serangan Siber Ancam Indonesia Sepanjang 2017”, OkeZone, 19 Desember 2017, [<https://techno.okezone.com/read/2017/12/19/207/1832777/205-juta-serangan-siber-ancam-indonesia-sepanjang-2017>].

Liana Threestayanti, “Gawat, Sudah 5 Tahun Kelompok Hacker Ini Serang Sistem Pemerintah”, Info Komputer, 12 Mei 2020, [<https://infokomputer.grid.id/read/122148047/gawat-sudah-5-tahun-kelompok-hacker-ini-serang-sistem-pemerintah>].

Lucky Maulana Firmansyah, “Indonesia Jadi Negara Dengan Serangan Siber Tertinggi”, Lokadata, 1 Juni 2020, [<https://lokadata.id/artikel/indonesia-jadi-negara-dengan-serangan-siber-tertinggi>].

Malay Mail, “Armed Forces To Set Up Cyber Unit”, 15 Januari 2020, [<https://www.malaymail.com/news/malaysia/2020/01/15/armed-forces-to-set-up-cyber-unit/1828332>].

Malaysia National Cyber Security Agency (NACSA), [<https://www.nacsa.gov.my>].

Matt Liebowitz, “Hackers Interfered With 2 US Government Satellites”, Space.com, 27 Oktober 2011, [<https://www.space.com/13423-hackers-government-satellites.html>].

Michael Raska dan Benjamin Ang, “Cybersecurity in Southeast Asia”, Asia Centre, 22 Mei 2018, [https://centreasia.eu/wp-content/uploads/2018/12>NotePre%CC%81 sentation-AngRaska-Cybersecurity_180518].

Microsoft Indonesia, “Ancaman Keamanan Siber Menyebabkan Kerugian Ekonomi bagi Organisasi di Indonesia Sebesar US\$34.2 Miliar”, 24 Mei 2018, [<https://news.microsoft.com/id-id/2018/05/24/ancaman-keamanan-siber>-

menyebabkan kerugian ekonomi bagi organisasi di Indonesia sebesar US\$34,2 miliar].

My ATM, “*Malaysian Armed Forces To Set Up Cyber Electromagnetic Command*”, Malaysia Military Times, 6 November 2019, [<https://mymilitarytimes.com/index.php/2019/11/06/malaysian-armed-forces-to-set-up-cyber-electromagnetic-command>].

Natsec, “*China-Based APT Mustang Panda Targets, Public and Private Sector Organizations*”, National Security, 7 Oktober 2019, [<https://natsec.medium.com/china-based-apt-mustang-panda-targets-public-and-private-sector-organizations>].

Noer Qomariah Kusumawardhani dan Rizy Suryarandika, “*Tren Teknologi dan Ancaman Siber Makin Ngeri di 2021*”, Republika Online, 2 Januari 2021, [<https://www.republika.co.id/berita/qlx390368/tren-teknologi-dan-ancaman-siber-makin-ngeri-di-2021>].

North Atlantic Treaty Organization (NATO), “*NATO's role in Kosovo*”, 16 November 2020, [https://www.nato.int/cps/en/natolive/topics_48818.htm].

Philippines Department of Information and Communications Technology (DICT), *Cybercrime Prevention Act of 2012*, [<https://dict.gov.ph/cybersecurity>]

Cybercrime Investigation and Coordinating Center (CICC), [<https://dict.gov.ph/cybercrime-investigation-and-coordinating-center-cicc>].

Prashanth Parameswaran, “*Thailand's Military to Set Up New Cyberwar Unit*”, The Diplomat, 22 Oktober 2015, [<https://thediplomat.com/2015/10/thailands-military-to-set-up-new-cyberwar-unit>].

Patrick Howell O'Neill, “*Pakistani military leverages Facebook Messenger for wide-ranging spyware campaign*”, Cyber Scoop, 15 Mei 2018, [<https://www.cyberscoop.com/pakistani-military-spyware-stealth-mango-tangelo-lookout>].

Pierluigi Paganini, “*Operation Shaheen – Pakistan Air Force members targeted by nation-state attackers*”, Security Affairs, 13 November 2018, [<https://securityaffairs.co/wordpress/77982/apt/operation-shaheen-campaign.html>].

Priam F. Nepomuceno, "AFP to create unit to defend PH military cyberspace", Bilyonaryo, 9 Juli 2017, [<https://bilyonaryo.com.ph/2017/07/09/afp-create-unit-defend-ph-military-cyberspace>].

Puspen TNI, "Panglima TNI: Satsiber TNI Melindungi Infrastruktur Kritis TNI", 18 Maret 2019, [<https://tni.mil.id/view-147370-panglima-tni-satsiber-tni-melindungi-infrastruktur-kritis-tni.html>].

Putri Zakia Salsabila, "Kejahanan Siber Di Indonesia Naik 4 Kali Lipat Selama Pandemi", Kompas, 12 Oktober 2020, [<https://tekno.kompas.com/read/2020/10/12/07020007/kejahanan-siber-di-indonesia-naik-4-kali-lipat-selama-pandemi>]

Reyn Gloria, "Bawaslu Tangani Ribuan Pelanggaran Netralitas ASN Saat Pemilu 2019", Badan Pengawas Pemilu (Bawaslu), 6 Juni 2019, [<https://bawaslu.go.id/id/berita/bawaslu-tangani-ribuan-pelanggaran-netralitas ASN-saat-pemilu-2019>].

Reuters, "Russia hacked Danish defense for two years, minister tells newspaper", 24 April 2017, [<https://www.reuters.com/article/us-denmark-security-russia-idUSKBN17P0NR>].

Rich Abbot, "Report: FireEye Says Chinese Hackers Attacking South Korea Over THAAD Deployment", Defense Daily, 5 Mei 2017, [<https://www.defensedaily.com/report-fireeye-says-chinese-hackers-attacking-south-korea-thaad-deployment-3/uncategorized>].

Robert M. Lee, et.al., "Analysis of the Cyber Attack on the Ukrainian Power Grid", SANS Industrial Control System dan Electricity Information Sharing and Analysis Center, 18 Maret 2016, diunduh dari [<http://ics.sans.org/duc5>].

Sandeep Joshi, "112 Government Websites Hacked In The Last 3 Months", The Hindu, 16 Maret 2012, [<https://www.thehindu.com/sci-tech/technology/internet/112-government-websites-hacked-in-the-last-3-months/article2999836.ece>].

Sean Lyngaas, "China-linked hackers have targeted Malaysian government, officials warn", Cyber Scoop, 6 Februari 2020, [<https://www.cyberscoop.com/china-malaysia-fireeye-kaspersky>].

Sindo News, "Proteksi Ekonomi Digital, Serangan Cyber di Indonesia Capai 232,4 Juta Kali", 26 April 2019,
[<https://ekbis.sindonews.com/berita/1399048/178/proteksi-ekonomi-digital-serangan-cyber-di-indonesia-capai-2324-juta-kali>].

Singapore Minister of Defence, "A Restructured SAF to Better Meet New Security Threats", Mindef, 2 Maret 2020,
[https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2020/March/02mar20_fs].

Tempo, "RUU KKS Resmi Dibatalkan", 27 September 2019,
[<https://nasional.tempo.co/read/1253198/ruu-kks-resmi-dibatalkan>].

The Armed Forces of the Philippines (AFP), "AFP to Strengthen Cyber Workforce", 9 Juli 2017, [<https://www.afp.mil.ph/index.php/news/8-afp-news/436-afp-to-strengthen-cyber-workforce>]

The Cylance Threat Intelligence Team, "The White Company: Inside the Operation Shaheen Espionage Campaign", BlackBerry Threat Vector, 18 November 2018, [<https://blogs.blackberry.com/en/2018/11/the-white-company-inside-the-operation-shaheen-espionage-campaign>].

The Straits Times, "Malaysia's Armed Forces Confirms Cyber-Attack On Network", 29 Desember 2020, [<https://www.straitstimes.com/asia/se-asia/malaysias-armed-forces-confirms-cyber-attack-on-network>].

The White House, A National Security Strategy For A New Century, 1998, U.S. National Security Strategy Archive [<https://nssarchive.us/national-security-strategy-1998>].

Thrina Tham, "SAF Ramps Up Counter-Terrorism Intelligence, Cyber And Maritime Capabilities", Pioneer, 2 Maret 2020,
[<https://www.mindef.gov.sg/web/portal/pioneer/article/feature-article-detail/ops-and-training>]

Times of India, "Pulwama attack: Pakistani websites hacked, here's the list", 18 Februari 2019, [<https://timesofindia.indiatimes.com/gadgets-news/pulwama-attack-pakistani-websites-hacked-heres-the-list>].

Times of Israel, "US conducted cyberattack on Iran following strike on Saudi oil – report", 16 Oktober 2019, [<https://www.timesofisrael.com/us-conducted-cyberattack-on-iran-following-strike-on-saudi-oil-report>].

Tom Westbrook, "Joint Strike Fighter plans stolen in Australia cyber attack", Reuters, 12 Oktober 2017, [<https://www.reuters.com/article/us-australia-defence-cyber-idUSKBN1CH00F>].

U.S. Cybersecurity and Infrastructure Security Agency (CISA), "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors", Alert (TA18-074A), 15 Maret 2018, [<https://us-cert.cisa.gov/ncas/alerts/TA18-074A>].

U.S. Department of Treasury, "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups", 13 September 2019, [<https://home.treasury.gov/news/press-releases/sm774>].

Warwick Ashford, "Norwegian healthcare breach alert failed GDPR requirements", Computer Weekly, 22 Januari 2018, [<https://www.computerweekly.com/news/252433538/Norwegian-healthcare-breach-alert-failed-GDPR-requirements>].

Yuswardi A. Suud, "Lima Tahun Tak Terdeteksi, Hacker China Ketahuan Mata-matai Indonesia dan Negara Asia Pasifik", Cyberthreat.id, 7 Mei 2020, [<https://cyberthreat.id/read/6554/Lima-Tahun-Tak-Terdeteksi-Hacker-China-Ketahuan-Mata-matai-Indonesia-dan-Negara-Asia-Pasifik>].

Zak Doffman, "U.S. Military Warns Outlook Users To Update Immediately Over Hack Linked To Iran", Forbes, 3 Juli 2019, [<https://www.forbes.com/sites/zakdoffman/2019/07/03/u-s-cyber-command-warns-millions-of-outlook-users-of-malicious-hack-linked-to-iran/?sh=636398526fd4>].

Zaid Shoorbajee, "Russians' stealthy 'LoJax' malware can infect on the firmware level", Cyber Scoop, 27 September 2017, [<https://www.cyberscoop.com/lojax-russia-apt28-eset-firmware>].

, "Potensi Serangan Siber Tahun 2020 Menurut BSSN", 23 Desember 2019, [<https://www.antaranews.com/berita/1220831/potensi-serangan-siber-pada-2020-menurut-bssn>].

_____, "BSSN sebut serangan siber bersifat sosial sangat berbahaya", 3 Februari 2021, [<https://www.antaranews.com/berita/1981266/bssn-sebut-serangan-siber-bersifat-sosial-sangat-berbahaya>].

_____, "Laporan Kinerja BSSN Tahun 2018 Beserta Manual Indikator Kinerja Utama (IKU)", [<https://bssn.go.id/laporan-kinerja-bssn-2018-beserta-manual-iku>].

_____, "Langkah BSSN Dalam Melakukan Deteksi Ancaman Siber", 7 Februari 2019, diunduh dari website BSSN [<https://bssn.go.id/press-release-honeynet-project-langkah-bssn-dalam-melakukan-deteksi-ancaman-siber>].

_____, "Mengenali Serangan Siber Global dan Nasional Melalui Laporan Tahunan Honeynet Project BSSN-IHP Tahun 2018", 8 Februari 2019, diunduh dari website BSSN [<https://bssn.go.id/mengenali-serangan-siber-global-dan-nasional-melalui-laporan-tahunan-honeynet-project-bssn-ihp-tahun-2018>].

_____, "BSSN Gelar Diskusi Publik dan Simposium Nasional RUU Keamanan dan Ketahanan Siber", [<https://bssn.go.id/press-release-bssn-gelar-diskusi-publik-dan-simposium-nasional-ruu-keamanan-dan-ketahanan-siber>].

_____, "Pusat Operasi Keamanan Siber Nasional", diakses dari [<https://bssn.go.id/pusat-operasi-keamanan-siber-nasional>].

_____, Laporan Tahunan Periode Januari-Desember 2019, [<https://bssn.go.id/laporan-tahunan-2019-pusopkamsinas-bssn>].

_____, "Laporan Tahunan 2019 Pusopkamsinas BSSN", 6 Maret 2020, [<https://bssn.go.id/laporan-tahunan-2019-pusopkamsinas-bssn>].

_____, "BSSN Gelar Webinar Peningkatan Kualitas Deteksi Ancaman Siber Melalui Pusat Malware Nasional", 14 Juli 2020, [<https://bssn.go.id/bssn-gelar-webinar-peningkatan-kualitas-deteksi-ancaman-siber-melalui-pusat-malware-nasional>].

_____, “Peran BSSN dalam Membangun Ekonomi Digital Indonesia”, 24 Juli 2020, diakses dari [<https://bssn.go.id/peran-bssn-dalam-membangun-ekonomi-digital-indonesia>].

_____, “Kepala BSSN: Strategi Keamanan Siber Nasional Juga Naungi Entitas Ekonomi Digital”, 22 Desember 2020, [<https://bssn.go.id/kepala-bssn-strategi-keamanan-siber-nasional-juga-naungi-entitas-ekonomi-digital>].

_____, Laporan Tahunan Hasil Monitoring Keamanan Siber Tahun 2020, [<https://bssn.go.id/bssn-publikasikan-hasil-monitoring-keamanan-siber-tahun-2020>].

_____, “Raker Dengan Komisi I DPR RI, BSSN: SNKS RI Sebagai Langkah Nyata Kehadiran Negara di Ruang Siber”, 3 Februari 2021, diakses dari [<https://bssn.go.id/raker-dengan-komisi-i-dpr-ri-bssn-snks-ri-sebagai-langkah-nyata-kehadiran-negara-di-ruang-siber>].

_____, “Seminar Nasional Cyber Warfare, Kasau: TNI AU Harus Berperan Aktif Hadapi Kejahatan Siber”, 14 November 2018, [<https://tni-au.mil.id/seminar-nasional-cyber-warfare-kasau-tni-au-harus-berperan-aktif-hadapi-kejahatan-siber>].

_____, “Resmikan Satsiber Dispamsanau, Kasau: Internet Berevolusi Menjadi Domain Sarana Untuk Pertempuran”, 18 September 2020, [<https://tni-au.mil.id/resmikan-satsiber-dispamsanau-kasau-internet-berevolusi-menjadi-domain>].

_____, Siaran Pers Nomor 66/HM/KOMINFO/03/2021 tentang Momentum Percepatan Transformasi Digital, 1 Maret 2021, [https://www.kominfo.go.id/content/detail/33022/siaran-pers-no-66hmkominfo032021-tentang-menkominfo-tegaskan-2021-momentum-percepatan-transformasi-digital/0/siaran_pers].

_____, Pidato Kenegaraan Presiden Joko Widodo Tahun 2019, 16 Agustus 2019, [<https://aptika.kominfo.go.id/2019/08/pidato-kenegaraan-presiden-jokowi-tahun-2019>].

_____, “RUU Keamanan dan Ketahanan Siber Dibatalkan”, 27 September 2019, [<https://nasional.kompas.com/read/2019/09/27/18241611/ruu-keamanan-dan-ketahanan-siber-dibatalkan>].

_____, “Kepala BSSN: Serangan Siber 2020 Meningkat 3 Kali Lipat”, 3 Februari 2021, [<https://nasional.kompas.com/read/2021/02/03/17415811/kepala-bssn-serangan-siber-2020-meningkat-3-kali-lipat>].

_____, “Pengguna Internet Indonesia Tembus 200 Juta, Hampir Semua Online Dari Ponsel”, 24 Februari 2021, [<https://tekno.kompas.com/read/2021/02/24/07020097/pengguna-internet-indonesia-tembus-200-juta-hampir-semua-online-dari-ponsel>].

_____, “What’s Behind Singapore’s New Integrated Military Cyber Command Objective?”, The Diplomat, 10 Maret 2020, [<https://thediplomat.com/2020/03/whats-behind-singapores-new-integrated-military-cyber-command-objective>].

_____, “US Cyber Command warns of Iran-linked hackers exploiting CVE-2017-11774 Outlook flaw”, Security Affairs, 3 Juli 2019, [<https://securityaffairs.co/wordpress/87895/breaking-news/cve-2017-11774-apt33-attacks.html>].

_____, “Vietnam’s neighbors, ASEAN, targeted by hackers: report”, Reuters, 7 November 2017, [<https://www.reuters.com/article/us-cyber-attack-vietnam-idUSKBN1D70VU>].

_____, “Kasus Malware Indonesia Tertinggi di Asia Pasifik pada 2019”, Tempo.co, 29 Juni 2020, diakses dari [<https://tekno,tempo.co/read/1358913/kasus-malware-indonesia-tertinggi-di-asia-pasifik-pada-2019>].

_____, “BSSN Gelar Bincang Strategi Keamanan Siber”, 22 Desember 2020, [<https://nasional,tempo.co/read/1416688/bssn-gelar-bincang-strategi-keamanan-siber>].



ALUR PIKIR
PENINGKATAN KEMAMPUAN SIBER TNI AU UNTUK MENDUKUNG
PENGAMANAN INFRASTRUKTUR STRATEGIS NASIONAL

POKOK PERSOALAN	INSTRUMENTAL INPUT	ENVIRONMENTAL INPUT
REGULASI YANG MENGATUR PERAN TNI DALAM MENANGGULANGI SERANGAN SIBER TERHADAP INFRASTRUKTUR STRATEGIS NASIONAL BELUM ADA.	- LANDASAN FILOSOFIS - LANDASAN TEORI - LANDASAN HUKUM - TINJAUAN PUSTAKA	UPAYA UNTUK MENINGKATKAN KEMAMPUAN SIBER TNI AU MELALUI REGULASI, ORGANISASI, SDM DAN SARPRAS
ORGANISASI SIBER TNI AU YANG MEMILIKI KEWENANGAN UNTUK BANTU PENGAMANAN INFRASTRUKTUR STRATEGIS NASIONAL BELUM ADA.		PERKEMBANGAN LINGKUNGAN STRATEGIS (GLOBAL, REGIONAL, NASIONAL, PELUANG DAN KENDALA)
KUANTITAS (JUMLAH) MAUPUN KUALITAS (KEMAMPUAN) PERSONEL TNI AU YANG MENGAWAKI SATUAN SIBER MASIH TERBATAS.		SARANA DAN PRASARANA TNI AU DALAM BIDANG SIBER YANG DIPERLUKAN UNTUK AMANKAN INFRASTRUKTUR STRATEGIS NASIONAL TERBATAS.



KEMAMPUAN SIBER
TNI AU SAATINI
MASIH TERBATAS

INFRASTRUKTUR
STRATEGIS
NASIONAL
AMAN

KEMAMPUAN SIBER
TNI AU PADA MASA
MENDATANG TELAH
MENINGKAT

**LAMPIRAN II TASKAP PENINGKATAN PUAN SIBER TNI AU
TANGGAL AGUSTUS 2021**

**LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA**

RIWAYAT HIDUP

DATA POKOK

1. NAMA : Donald Kasenda, S.T., S.I.P., M.M.
2. PANGKAT : Marsekal Pertama TNI
3. KORPS/PROF : Penerbang/Angkut
4. NRP : 515587
5. TANGGAL LAHIR : 8 Oktober 1970
6. TEMPAT LAHIR : Minahasa
7. AGAMA : Kristen Protestan

PENDIDIKAN UMUM

1. SD Negeri 1 Modoinding 1981
2. SMP Negeri 1 Modoinding 1984
3. SMA Kristen YPKM Manado 1988
4. S-1 Teknik Industri Universitas Suryadarma Jakarta 2001
5. S-1 Ilmu Politik Universitas Terbuka Jakarta 2002
6. S-2 Ilmu Manajemen Universitas Suryadarma Jakarta 2009

DIKMA / DIKBANGUM

1. AAU 1991
2. Sekkau ANGKATAN 67 2000
3. Seskoau ANGKATAN 43 2005
4. Maktab Turus ATM Malaysia ANGKATAN 39 2007
5. Sesko TNI ANGKATAN 43 2016

PENDIDIKAN MILITER (KURSUS)

1. Penataran P4	1991
2. Sarcab	1992
3. Sekbang	1994
4. Simulator Terbang di Belanda	1996
5. Konversi Terbang Pesawat SF-260 Marchetti di Singapura	2003

RIWAYAT KEPANGKATAN

27-07-1991	Letnan Dua
01-10-1994	Letnan Satu
01-10-1997	Kapten
01-10-2002	Mayor
01-10-2006	Letnan Kolonel
01-10-2011	Kolonel
29-04-2019	Marsekal Pertama TNI

RIWAYAT JABATAN

1. Pama DP AAU	1991
2. Pama DP Lanud Adisutjipto	1992
3. Pa Penerbang Skadron Udara 2 Lanud Lanud Halim P.	1994
4. Kapok Banhar Sihar Flighthar Skadron Udara 2 Lanud Halim P.	1995
5. Instruktur Penerbang Wingdik Terbang Lanud Adisutjipto	2004
6. Kadisops Skadron Udara 2 Lanud Halim P.	2004
7. Kasi Lambangja Wing 1 Lanud Halim P.	2006
8. Kasi Opslat Disops Lanud Halim P.	2007
9. Komandan Skadron Udara 2 Lanud Halim.	2009
10. Pabandya 2/Dalops Paban IV/Ops Sosp TNI	2010
11. Asops Kosekhanudnas III Medan	2011
12. Atase Udara RI di Belanda	2011
13. Dosen Utama Seskoau	2016
14. Paban II/Hublu Sintel Mabes TNI	2017
15. Kadispamsanau	2019

16. Komandan Lanud Manuhua Biak

2021

PENUGASAN

1. Latma Elang Malindo di Malaysia	1995
2. Latma Elang Ausindo di Australia	1996
3. Latma Elang Indopura di Singapura	1997
4. Latma Elang Thainesia di Thailand	1998
5. Latma Elang Brunesia di Brunei Darussalam	1999
6. Latma TNI AU dengan Filipina	2000

TANDA JASA / KEHORMATAN

1. Satyalencana Kesetiaan VIII Tahun.
2. Satyalencana Dharma Nusa.
3. Satyalencana Dwidja Sistha.
4. Satyalencana Kesetiaan XVI Tahun.
5. Bintang Yudha Dharma Nararya.
6. Bintang Swa Bhawana Paksa Nararya.
7. Satyalencana Kesetiaan XXIV Tahun.
8. Satyalencana Wira Nusa.

Jakarta, 25 Agustus 2021

Peserta,



Donald Kasenda, S.T., S.I.P., M.M.

Marsekal Pertama TNI