Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora
Volume 5, Nomor 2, April 2026
E-ISSN .: 2828-7622; P-ISSN .: 2828-7630, Hal. 665-673
DOI: https://doi.org/10.55606/jurrish.v5i2.7731
Tersedia: https://prin.or.id/index.php/JURRISH

Integrasi Pertahanan Siber dalam Sistem Pertahanan dan Keamanan Rakyat Semesta (Sishankamrata): Analisis Komparatif dengan Amerika Serikat, Estonia, dan Singapura

Wisanggeni Sholata Sya[1*], Herlina Tarigan[2], Susanto[3]
[1-3]Program Studi Manajemen Pertahanan, Universitas Pertahanan Republik Indonesia, Indonesia
Email: wisanggenisholatasya@gmail.com[1], herlin8@yahoo.com[2], efgh@gmail.com[3]*
**Penulis Korespondensi: wisanggenisholatasya@gmail.com*

Abstract. *Modern conflict has evolved into the cyber domain as part of hybrid warfare, demanding a reinterpretation of the Sishankamrata (Total People's Defense and Security System) doctrine to encompass the digital realm. This study aims to analyze the integration of cyber defense into the Sishankamrata framework using a literature review and comparative analysis with the cyber defense strategies of the United States, Estonia, and Singapore. The results indicate that the implementation of Sishankamrata in the cyber domain faces challenges regarding inter-institutional synergy and unclear operational roles for the Reserve and Support Components. Based on the comparative analysis, Estonia's Cyber Defence Unit model and Singapore's Digital Defence pillar are identified as the most effective blueprints for Indonesia to mobilize civilian experts and enhance social resilience. This study recommends that the government formalize "Digital Defense" as an integral pillar of Sishankamrata, establish a Cyber Reserve Component consisting of expert civilian volunteers, and strengthen legal frameworks and public digital literacy as a form of state defense.*

Keywords*: Cyber Defense; Hybrid Warfare; National Security; Sishankamrata; Total Defence.*

Abstrak. Konflik modern telah berkembang ke ranah siber sebagai bagian dari perang hibrida, yang menuntut penafsiran ulang doktrin Sistem Pertahanan dan Keamanan Rakyat Semesta (Sishankamrata) agar mencakup domain digital. Penelitian ini bertujuan menganalisis integrasi pertahanan siber ke dalam kerangka Sishankamrata melalui metode studi literatur dan analisis komparatif dengan strategi pertahanan siber Amerika Serikat, Estonia, dan Singapura. Hasil penelitian menunjukkan bahwa implementasi Sishankamrata di ranah siber masih menghadapi tantangan sinergi antarlembaga dan ketidakjelasan peran operasional Komponen Cadangan serta Komponen Pendukung. Berdasarkan analisis komparatif, model Cyber Defence Unit Estonia dan pilar Digital Defence Singapura diidentifikasi sebagai cetak biru paling efektif untuk Indonesia dalam memobilisasi ahli sipil dan meningkatkan ketahanan sosial. Penelitian ini merekomendasikan pemerintah untuk memformalkan "Pertahanan Digital" sebagai pilar integral Sishankamrata, membentuk Komponen Cadangan Siber yang terdiri dari relawan ahli sipil, serta memperkuat kerangka hukum dan literasi digital masyarakat sebagai bentuk bela negara

Kata kunci: Keamanan Nasional; Perang Hibrida; Pertahanan Siber; Pertahanan Total; Sishankamrata.

1. LATAR BELAKANG

Konflik modern tidak lagi terbatas pada domain darat, laut, dan udara. Kemunculan domain siber sebagai arena kelima telah menghadirkan tantangan sekaligus kerentanan baru bagi kedaulatan negara (Clarke & Knake, 2019). Serangan siber, baik yang dilancarkan oleh aktor negara maupun non-negara, dapat melumpuhkan infrastruktur kritis, mencuri data strategis, hingga mengobarkan perang informasi yang merusak tatanan sosial (BSSN, 2021). Fenomena ini dikenal sebagai bagian dari Perang Hibrida, di mana ranah siber digunakan sebagai instrumen destabilisasi non-kinetik (Hidayat, 2022).

Bagi Indonesia, yang mengadopsi doktrin Sistem Pertahanan dan Keamanan Rakyat Semesta (Sishankamrata), ancaman ini memerlukan penafsiran ulang tentang konsep "semesta"

Naskah Masuk: 07 November 2025; Revisi: 30 November 2025; Diterima: 27 Desember 2025;
Tersedia: 30 Desember 2025

yang kini juga mencakup ranah digital. Reinterpretasi ini mendesak karena infrastruktur kritis nasional—mulai dari energi, keuangan, hingga transportasi—kini sangat bergantung pada jaringan digital yang rentan (BSSN, 2021). Sishankamrata adalah doktrin pertahanan yang melibatkan seluruh sumber daya nasional—militer dan nirmiliter—untuk menghadapi ancaman (Kementerian Pertahanan Republik Indonesia, 2020).

Filosofi dasarnya adalah pengerahan kekuatan rakyat sebagai basis pertahanan. Namun, bagaimana doktrin yang berakar pada konsep perang teritorial ini beradaptasi dengan ancaman siber yang tidak mengenal batas wilayah, menjadi gap analysis sekaligus urgensi penelitian ini. Artikel ini bertujuan untuk menganalisis bagaimana pertahanan siber diintegrasikan ke dalam kerangka Sishankamrata. Selanjutnya, untuk mendapatkan perspektif yang lebih luas, strategi Indonesia akan dibandingkan dengan pendekatan yang diadopsi oleh Amerika Serikat, Estonia, dan Singapura.

2. KAJIAN TEORITIS

Teori Keamanan Komprehensif dan Pertahanan Total

Konsep Sishankamrata di Indonesia berakar kuat pada kerangka Keamanan Komprehensif (*Comprehensive Security*) dan Pertahanan Total (*Total Defence*). Teori Pertahanan Total berpendapat bahwa menghadapi ancaman kedaulatan memerlukan mobilisasi seluruh elemen masyarakat dan sumber daya nasional, melampaui kemampuan militer semata (Rid, 2020). Doktrin ini menekankan adanya tanggung jawab kolektif masyarakat sipil untuk mendukung pertahanan negara, baik dalam domain fisik maupun non-fisik.

Sistem Pertahanan dan Keamanan Rakyat Semesta (Sishankamrata)

Indonesia menganut sistem pertahanan keamanan rakyat semesta (Sishankamrata) sebagai doktrin utama dalam menjaga kedaulatan dan kepentingan nasional. Pertahanan nasional tidak hanya pada aspek fisik melalui pertahanan militer dalam menghadapi ancaman militer dan pertahanan nirmiliter dan hibrida termasuk aspek strategis termasuk ideology, politik, ekonomi, sosial, budaya serta keamanan (Purwantoro, 2025).

Sishankamrata, yang diamanatkan oleh UUD 1945 Pasal 30, adalah sistem pertahanan yang bersifat semesta, melibatkan seluruh warga negara, wilayah, dan sumber daya nasional lainnya (Kemhan, 2020). Sistem ini terdiri dari tiga komponen:

1) Komponen Utama: Tentara Nasional Indonesia (TNI) dan Kepolisian Negara Republik Indonesia (Polri). Di ranah siber, TNI mengembangkan kapabilitas melalui unit-unit khusus seperti Satuan Siber (Satsiber) TNI untuk operasi pertahanan militer (Markas Besar TNI, 2021).

2) Komponen Cadangan: Sumber daya nasional yang telah disiapkan untuk dikerahkan guna memperbesar kekuatan Komponen Utama.
3) Komponen Pendukung: Sumber daya nasional yang dapat digunakan untuk meningkatkan kekuatan dan kemampuan Komponen Utama dan Komponen Cadangan, mencakup warga negara, aparatur sipil negara, sektor swasta, dan elemen masyarakat lainnya.

   Secara tradisional, fokus Sishankamrata adalah pada pertahanan teritorial untuk melawan agresi militer konvensional. Tantangan saat ini adalah menerjemahkan partisipasi Komponen Cadangan dan Pendukung dari konteks perang teritorial ke dalam konteks ancaman siber yang sangat teknis (Nugroho & Kusuma, 2022).

Pertahanan Siber dalam Konteks Perang Hibrida

Perang Hibrida (*Hybrid Warfare*) merupakan perang yang menggabungkan teknik perang konvensional, perang asimetris, dan perang informasi untuk mendapatkan kemenangan atas pihak lawan (Duarte, 2025). Dalam perang hibrida, negara menggunakan kombinasi strategi militer dan nirmiliter untuk mencapai tujuan mereka. Taktik-taktik yang digunakan, meliputi penggunaan kekuatan militer konvensional, serangan siber, propaganda, maneuver politik dan diplomatik, intervensi ekonomi, atau kekerasan nirmiliter lainnya untuk mempengaruhi musuh dan mencapai tujuan politik atau militer mereka (Saragih, 2025). Domain siber menjadi elemen kunci dalam perang hibrida karena memungkinkan serangan yang bersifat asimetris, anonim, murah, dan sulit diatributkan, namun memiliki dampak destabilisasi yang masif (Tapsell, 2021). Dalam konteks ini, pertahanan siber mencakup tindakan proaktif dan reaktif untuk melindungi infrastruktur informasi kritis, serta menanggapi insiden siber. Pertahanan siber yang efektif dalam kerangka Pertahanan Total harus melibatkan edukasi dan ketahanan sosial terhadap disinformasi dan propaganda untuk melemahkan moral bangsa (Wibowo, 2022).

Ulasan Penelitian Terdahulu dan Research Gap

Penelitian mengenai integrasi siber dalam Sishankamrata telah mengidentifikasi tantangan struktural. Nugroho dan Kusuma (2022) menyoroti kebutuhan strategis untuk membentuk Komponen Cadangan Siber yang efektif, namun mencatat bahwa kerangka hukum dan operasionalnya belum terbentuk. Sementara itu, Pratama (2023) dan Susilo (2023) secara terpisah menganalisis masalah sinergi dan tata kelola antarlembaga pertahanan siber di Indonesia, khususnya antara BSSN dan TNI, menyimpulkan bahwa pembagian peran yang belum jelas masih menjadi diskursus yang terus berkembang. Saraswati (2021) juga

menekankan bahwa perlindungan infrastruktur siber kritis masih membutuhkan kerangka hukum yang lebih komprehensif.

Research gap yang ditawarkan penelitian ini adalah melakukan analisis komparatif yang terperinci dengan negara-negara yang telah berhasil mengoperasionalkan konsep Pertahanan Total/Komprehensif di ranah siber yaitu Amerika Serikat, Estonia dan Singapura, untuk mengekstrak model implementasi yang dapat digunakan sebagai cetak biru untuk mengatasi tantangan internal yang telah diidentifikasi oleh peneliti sebelumnya.

3. METODE PENELITIAN

Penelitian ini menggunakan metode studi literatur dan analisis komparatif. Data dikumpulkan melalui kajian mendalam terhadap dokumen-dokumen kebijakan resmi terkait Sishankamrata, undang-undang terkait keamanan siber, serta jurnal ilmiah dan publikasi yang relevan. Analisis Komparatif dilakukan untuk membandingkan strategi dan implementasi pertahanan siber Indonesia dalam kerangka Sishankamrata dengan model yang diterapkan oleh Amerika Serikat, Estonia, dan Singapura. Perbandingan ini bertujuan untuk mengidentifikasi kekuatan, tantangan, dan celah dalam implementasi Sishankamrata di domain siber, yang kemudian digunakan sebagai dasar untuk merumuskan rekomendasi strategis.

4. HASIL DAN PEMBAHASAN

Hasil Analisis Komparatif Strategi Pertahanan Siber

1) *Indonesia: Pertahanan Siber dalam Kerangka Sishankamrata*

   Pertahanan siber Indonesia secara kelembagaan dipimpin oleh Badan Siber dan Sandi Negara (BSSN) untuk ranah sipil dan diperkuat oleh unit-unit siber di bawah TNI untuk ranah militer (BSSN, 2021; Markas Besar TNI, 2021). Konsep Sishankamrata memiliki potensi besar untuk memobilisasi "rakyat" sebagai *firewall* manusia. Namun, sinergi dan pembagian peran yang jelas antar lembaga ini masih menjadi diskursus yang terus berkembang (Pratama, 2023). Peran Komponen Cadangan dan Pendukung dalam konteks siber belum terdefinisi secara jelas dan operasional (Nugroho & Kusuma, 2022).

2) *Amerika Serikat: Doktrin Defend Forward*

   Amerika Serikat mengadopsi strategi siber yang proaktif, dikenal dengan istilah "*defend forward*" atau pertahanan ke depan (The White House, 2023). Pendekatan ini menekankan pada tindakan mengganggu dan menghalangi aktivitas siber musuh di jaringan mereka, sebelum mencapai jaringan AS. Strategi ini sebagian besar dibentuk

oleh persaingan strategis yang disebut sebagai '*persistent engagement*' (Rid, 2020). Struktur utamanya adalah *United States Cyber Command* (USCYBERCOM), yang berfokus pada proyeksi kekuatan siber global, bukan mobilisasi pertahanan rakyat.

3) *Estonia: Ketahanan Siber Seluruh Masyarakat*

Setelah mengalami serangan siber besar-besaran pada tahun 2007, Estonia membangun ekosistem pertahanan siber yang sangat bergantung pada ketahanan seluruh lapisan masyarakat (Schmidt, 2013). Mereka memiliki *Cyber Defence Unit* (CDU), sebuah organisasi paramiliter sukarela yang terdiri dari para profesional TI dari sektor swasta yang siap dimobilisasi saat krisis. CDU adalah contoh nyata bagaimana Komponen Cadangan dan Pendukung dapat diorganisir secara efektif untuk pertahanan siber. Model Estonia adalah implementasi Sishankamrata di ranah siber yang paling mendekati, dengan memformalkan peran para sukarelawan ahli.

4) *Singapura: Pertahanan Digital sebagai Pilar Pertahanan Total*

Singapura, yang menganut konsep *Total Defence*, secara resmi menambahkan *Digital Defence* (Pertahanan Digital) sebagai pilar keenam pada tahun 2019 (*Ministry of Defence Singapore* [MINDEF], 2019). Ini adalah pengakuan eksplisit bahwa domain digital adalah bagian integral dari keamanan nasional. Pertahanan Digital mencakup keamanan siber untuk melawan serangan teknis dan ketahanan terhadap misinformasi dan berita palsu. Setiap individu dipandang sebagai garis pertahanan pertama (Tapsell, 2021). Pendekatan Singapura menawarkan cetak biru yang jelas bagi Indonesia tentang bagaimana mengartikulasikan pertahanan siber sebagai tanggung jawab bersama.

Tabel 1. Perbandingan Model Pertahanan Siber Nasional.

(Diolah dari: Kemhan, 2020; The White House, 2023; Schmidt, 2013; MINDEF, 2019)

Aspek Kunci	Indonesia (Sishankamrata)	Amerika Serikat	Estonia	Singapura (*Total Defence*)
Doktrin Utama	Defensif, berbasis kerakyatan	Ofensif, pertahanan ke depan (*Defend Forward*)	Defensif, ketahanan seluruh masyarakat	Defensif, tanggung jawab bersama
Pilar Explicit Siber	Belum ada pilar eksplisit	Fokus pada Militer (USCYBERCOM)	Unit Pertahanan Siber (CDU)	Pertahanan Digital (Pilar Keenam)

Aspek Kunci	Indonesia (Sishankamrata)	Amerika Serikat	Estonia	Singapura (*Total Defence*)
Peran Warga Negara	Komponen Pendukung (belum terdefinisi jelas)	Kemitraan Swasta/Edukasi Individu	Relawan Ahli terorganisir (CDU)	Garis pertahanan pertama (melawan *fake news* & *cyber hygiene*)
Kekuatan Kunci	Potensi mobilisasi massa dan filosofi semesta	Kapabilitas ofensif, teknologi superior	Integrasi sipil-militer yang kuat, ketahanan sosial	Kejelasan doktrin dan kampanye publik efektif

Pembahasan: Relevansi dan Tantangan Adaptasi Sishankamrata di Domain Siber

1) Sinkronisasi dengan Literatur dan Isu Sentral

Temuan bahwa peran Komponen Cadangan dan Pendukung Indonesia belum terdefinisi secara operasional mengkonfirmasi kesimpulan dari Nugroho dan Kusuma (2022) tentang kebutuhan mendesak akan Komponen Cadangan Siber. Model Estonia melalui CDU, yang memobilisasi ahli TI sipil sebagai paramiliter sukarela, memberikan cetak biru paling relevan bagi Indonesia. Selain itu, kurangnya sinergi kelembagaan di Indonesia seperti yang diulas oleh Pratama (2023) dan Susilo (2023) dapat diatasi dengan mengadopsi pendekatan Pilar Pertahanan Digital Singapura. Penambahan pilar ini akan memastikan bahwa pertahanan siber tidak hanya dilihat sebagai tugas teknis BSSN atau militer TNI, tetapi sebagai tanggung jawab lintas sektor.

2) Implikasi Teoritis

Secara teoritis, temuan ini menggarisbawahi perlunya evolusi doktrin Pertahanan Total di era Perang Hibrida. Konsep "semesta" dalam Sishankamrata tidak lagi hanya merujuk pada cakupan geografis, tetapi juga pada cakupan domain ancaman. Keberhasilan Singapura dan Estonia menunjukkan bahwa teori Pertahanan Total hanya relevan jika dimutakhirkan dengan pilar-pilar yang berorientasi pada ancaman non-fisik (Rid, 2020).

3) Implikasi Praktis (Kebijakan)

Secara praktis, hasil komparatif ini menawarkan rekomendasi implementatif yang didukung oleh analisis negara pembanding:

a) Mengadopsi Model Proaktif: Walaupun Indonesia bersifat defensif, kemampuan AS (*Defend Forward*) menyoroti pentingnya kapabilitas siber ofensif yang terintegrasi di bawah TNI untuk tujuan penangkalan. Kebijakan pertahanan siber Indonesia perlu menyertakan spektrum operasi siber penuh, tidak hanya defensif, untuk menjaga kredibilitas penangkalan (The White House, 2023).
b) Formalisasi Komponen Cadangan Siber (Model Estonia): Pemerintah harus segera merumuskan Peraturan Pemerintah (PP) atau Peraturan Presiden (Perpres) yang mengatur pembentukan dan operasionalisasi Komponen Cadangan Siber yang terdiri dari ahli sipil, untuk mendukung Komponen Utama saat krisis siber. Hal ini sangat penting untuk menjembatani kesenjangan SDM antara kebutuhan dan ketersediaan, sesuai yang diulas oleh Nugroho dan Kusuma (2022).
c) Penguatan Kerangka Hukum Siber: Perlu adanya penyelarasan regulasi antara UU Perlindungan Data Pribadi dan regulasi keamanan siber lainnya untuk memberikan kejelasan wewenang (Pratama, 2023). Arsitektur hukum yang komprehensif adalah prasyarat bagi efektivitas pertahanan siber di Indonesia (Saraswati, 2021).
d) Literasi Digital sebagai Bela Negara (Model Singapura): Bela negara harus diimplementasikan melalui kampanye literasi digital yang masif sebagai bagian dari peran Komponen Pendukung. Hal ini adalah garis pertahanan pertama melawan disinformasi (*fake news*) dan menumbuhkan *cyber hygiene* (Wibowo, 2022).

5. KESIMPULAN DAN SARAN

Doktrin Sishankamrata secara filosofis sangat ideal untuk membangun pertahanan siber nasional yang tangguh karena menekankan pada pengerahan seluruh kekuatan bangsa. Namun, dalam praktiknya, implementasi pertahanan siber Indonesia masih menghadapi tantangan utama dalam sinergi antarlembaga (Susilo, 2023) dan formalisasi peran Komponen Cadangan serta Komponen Pendukung di ranah digital. Sishankamrata memiliki potensi besar untuk ketahanan siber, tetapi membutuhkan artikulasi doktrinal yang eksplisit terhadap ancaman siber, seperti model Pilar Pertahanan Digital Singapura (MINDEF, 2019). Model Estonia dan Singapura terbukti paling efektif dalam menerjemahkan konsep Pertahanan Total ke dalam aksi siber nyata, terutama dalam hal mobilisasi masyarakat dan tenaga ahli.

Berdasarkan hasil penelitian, penulis memberikan saran dan rekomendasi sebagai berikut:

a. Pemerintah perlu secara eksplisit menambahkan "Pertahanan Digital" sebagai bagian integral Sishankamrata sebagai bentuk Formalisasi Pilar Pertahanan Digital,
b. Pemerintah perlu mengembangkan kerangka kerja hukum dan operasional yang formal untuk membentuk Komponen Cadangan Siber, meniru model relawan ahli Estonia, sebagaimana disarankan oleh Nugroho dan Kusuma (2022),
c. Pemerintah perlu menyelaraskan regulasi untuk memberikan kejelasan wewenang dalam tata kelola siber sebagai bentuk penguatan kerangka hukum.
d. Pemerintah dan lembaga terkait harus mengintensifkan edukasi publik sebagai implementasi peran Komponen Pendukung seperti literati digital sebagai bentuk bela negara.

DAFTAR REFERENSI

Adma, A., Surbakti, Y. M., & Sari, P. (2023). Transformasi sistem pertahanan siber Indonesia dengan BSSN sebagai poros dan motor penggerak menuju angkatan siber mandiri di masa depan. *Jurnal Kajian Stratejik Ketahanan Nasional, 6*(1), 107–124. https://doi.org/10.7454/jkskn.v6i1.10077

Badan Siber dan Sandi Negara. (2021). *Lanskap ancaman siber Indonesia dan strategi perlindungan infrastruktur kritis nasional*. BSSN RI.

Bhakti, A., Sudirman, A., Sumadinata, R. W. S., & Bainus, A. (2024). State defense strategy in facing cyber threats after hacking incidents on government institutions: A case study in Indonesia. *Journal of Human Security, 20*(1), 109–117.

Bua, I. T., & Idris, N. I. (2025). Analisis kebijakan keamanan siber di Indonesia: Studi kasus kebocoran data nasional pada tahun 2024. *Desentralisasi: Jurnal Hukum, Kebijakan Publik, dan Pemerintahan, 2*(2), 100–114. https://doi.org/10.62383/desentralisasi.v2i2.653

Clarke, R. A., & Knake, R. K. (2019). *The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats*. Penguin Press.

Darumaya, B. A., Maarif, S., Toruan, T. S. L., & Swastanto, Y. (2023). Pemikiran potensial ancaman perang siber di Indonesia: Suatu kajian strategi pertahanan. *Jurnal Keamanan Nasional, 9*(2), 299–324.

Duarte, E. P. (2025). *Manajemen pertahanan Indonesia dalam konteks kebijakan Trump: Analisis dan refleksi*. Indonesia Emas Group.

Hidayat, A. (2022). Perang hibrida dan masa depan sishankamrata. *Jurnal Studi Pertahanan, 8*(1), 45–60.

Kementerian Pertahanan Republik Indonesia. (2020). *Buku putih pertahanan Indonesia*. Kementerian Pertahanan RI.

Markas Besar TNI. (2021). *Doktrin pertahanan siber TNI*. Mabes TNI.

Ministry of Defence Singapore. (2019). *Digital defence: The sixth pillar of total defence*. MINDEF Communications Organisation. https://www.mindef.gov.sg/oms/totaldefence/digital-defence.html

Nugroho, B., & Kusuma, D. (2022). Membangun komponen cadangan siber: Tantangan dan peluang dalam konteks sishankamrata. *Jurnal Studi Strategis Indonesia, 7*(2), 145–160.

Pratama, R. A. (2023). Sinergi BSSN dan TNI dalam menghadapi ancaman siber: Sebuah tinjauan tata kelola. *Jurnal Pertahanan & Bela Negara, 13*(1), 88–102.

Purwantoro, S. D. (2025). *Manajemen pertahanan Indonesia dalam konteks kebijakan Trump: Analisis dan refleksi*. Indonesia Emas Group.

Ramadhan, T., Pujianto, R., & Santoso, F. B. (2024). Strategi penanganan keamanan siber di Indonesia. *JI-40: Journal of Informatics and Information Security, 5*(2), 183–192. https://doi.org/10.31599/v0xr7273

Rid, T. (2020). The great cyber competition. *Journal of Strategic Studies, 43*(2), 112–134.

Saragih, H. J. R. (2024). *MSDM pertahanan modern: Konsep dan implementasinya*. Indonesia Emas Group.

Saraswati, L. M. (2021). Arsitektur hukum keamanan siber Indonesia: Antara kedaulatan data dan keamanan nasional. Dalam A. B. Rahardjo & F. Maulana (Eds.), *Tata kelola siber di era digital* (hlm. 112–130). UI Press.

Schmidt, A. (2013). The 2007 cyber attacks on Estonia: Learning from a crisis. Dalam N. M. Wingfield & T. R. Johnson (Eds.), *Cyber power and national security* (hlm. 45–62). Potomac Books.

Susilo, A. B. (2023). Koordinasi kelembagaan dalam arsitektur pertahanan siber nasional: Tantangan dan prospek. *Jurnal Studi Keamanan Internasional, 15*(2), 112–128.

Tapsell, R. (2021). *The digital frontier: Disinformation and state power in Southeast Asia*. ANU Press. https://doi.org/10.1007/978-981-15-5876-4_7

The White House. (2023). *National cybersecurity strategy*. The White House. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Wibowo, S. (2022). Ketahanan sosio-kultural sebagai respon terhadap ancaman non-militer. *Jurnal Ketahanan Nasional, 28*(3), 301–318.