

## **Model C6ISR Nasional Malaysia: Ancaman hibrid, jurang institusi dan pengajaran antarabangsa**

Dzeidee Schaff Jamaludin, Mohd Ikbal Mohd Huda

Pusat Kajian Sejarah, Politik dan Hal Ehwal Antarabangsa,  
Fakulti Sains Sosial dan Kemanusiaan, Universiti Kebangsaan Malaysia

Correspondence: Mohd Ikbal Mohd Huda (e-mail: [ibahuda@ukm.edu.my](mailto:ibahuda@ukm.edu.my))

Received: 20 January 2026; Accepted: 11 March 2026; Published: 21 May 2026

### **Abstrak**

Ancaman hibrid dan cabaran keselamatan multi domain terus mendedahkan kelemahan struktur dalam ekosistem keselamatan negara, khususnya dari segi penyepaduan fungsi risikan, pemantauan dan perintah antara agensi. Kajian ini meneliti jurang institusi tersebut dan membangunkan satu model konseptual C6ISR iaitu *command, control, communications, computers, cyber, combat systems, intelligence, surveillance and reconnaissance* yang sesuai dengan konteks operasi Malaysia. Menggunakan reka bentuk kualitatif berasaskan analisis dokumen, kajian menilai dokumen dasar utama negara, laporan keselamatan serantau serta literatur antarabangsa mengenai C4ISR, operasi multi domain, GEOINT dan governans keselamatan. Analisis tematik mengenal pasti tiga isu utama: struktur perintah yang terfragmentasi, tahap interoperabiliti yang terhad antara agensi pertahanan dan awam serta ketiadaan rangka kerja *data fusion* dan *Common Operating Picture (COP)* pada peringkat nasional. Perbandingan dengan Amerika Syarikat, Singapura, Korea Selatan dan Turkiye menunjukkan bahawa keberkesanan C6ISR bergantung pada kerangka governans yang jelas, ekosistem data bersepadu dan mekanisme sokongan keputusan masa nyata. Dapatan ini memberikan asas kepada pemahaman tentang reformasi struktur yang diperlukan Malaysia bagi meningkatkan keupayaan koordinasi dalam operasi kompleks seperti keselamatan sempadan, insiden siber dan pemantauan domain maritim. Kajian ini mencadangkan satu model C6ISR konseptual yang merangkumi komponen penyepaduan perintah, *data fusion*, koordinasi rentas domain dan penjajaran institusi. Model ini berfungsi sebagai kerangka awal untuk memperkukuh governans keselamatan negara dan menyokong respon multi domain yang lebih koheren.

**Kata kunci:** Ancaman hibrid, C6ISR, governans keselamatan, keselamatan multi domain, Malaysia

## **Malaysian National C6ISR model: Hybrid threats, institutional gaps and international lessons**

### **Abstract**

Hybrid threats and multidomain security challenges continue to expose structural vulnerabilities in Malaysia's national security architecture, particularly in the integration of

intelligence, surveillance and command functions across agencies. This study examines these institutional gaps and proposes a conceptual C6ISR, namely command, control, communications, computers, cyber, combat systems, intelligence, surveillance and reconnaissance, model suited to Malaysia's operational context. Using a qualitative design based on document analysis, the research reviews key national policy documents, regional security reports and international literature on C4ISR, multidomain operations, GEOINT and security governance. The thematic analysis identifies three persistent issues: fragmented command structures, limited interoperability between defence and civilian agencies, and the absence of a national-level data fusion and Common Operating Picture (COP) framework. Comparative insights from the United States, Singapore, South Korea and Turkiye show that effective C6ISR systems rely on clear governance arrangements, integrated data ecosystems and real-time decision-support mechanisms. These cases provide reference points for understanding the structural reforms Malaysia requires to enhance its coordination capacity during complex operations such as border security, cyber incidents and maritime domain awareness. The study proposes a conceptual C6ISR model that outlines the essential components of command integration, data fusion, cross-domain coordination and institutional alignment. This model serves as an initial framework for strengthening Malaysia's security governance and supporting more coherent multidomain responses. The study contributes to the literature by situating C6ISR not only as a technological capability but as a governance challenge that requires organisational integration, strategic clarity and systemwide interoperability.

**Keywords:** Hybrid threats, C6ISR, security governance, multidomain security, Malaysia

## Pengelasan

Keselamatan nasional Malaysia kini dipengaruhi oleh evolusi ancaman hibrid yang beroperasi merentasi domain fizikal, digital dan kognitif secara serentak. Ancaman ini tidak lagi berbentuk tradisional, sebaliknya menggabungkan tekanan maritim, serangan siber, aktiviti pengaruh maklumat serta manipulasi geoekonomi yang saling bertindih. Hoffman (2007) menegaskan bahawa ancaman hibrid bersifat adaptif dan sukar diramal kerana ia menggabungkan unsur ketenteraan, bukan ketenteraan dan teknologi dalam satu ruang tindakan yang fleksibel. Di rantau Indo-Pasifik pula, persaingan kuasa besar menjadikan landskap keselamatan Malaysia lebih kompleks, khususnya di kawasan berkepentingan strategik seperti Laut China Selatan (Alatas, 2016; Lai & Kuik, 2020).

Dalam konteks ini, keupayaan sesebuah negara memahami gambaran situasi keseluruhan bergantung kepada tahap integrasi maklumat dan kecekapan sistem perintah serta kawalan yang menyelaraskan tindakan rentas domain. Perkembangan teori keselamatan moden seperti Securitisation Theory (Buzan, Wæver & De Wilde, 1998), Network Centric Warfare (Alberts & Hayes, 2006) dan Multi-Domain Operations (Joint Chiefs of Staff, 2018) menunjukkan bahawa pengurusan ancaman kontemporari tidak lagi bergantung kepada kapasiti fizikal semata-mata, tetapi kepada kebolehan menyepadukan data, risikan dan komunikasi dalam satu kerangka operasi yang bersifat nasional.

Walaupun Malaysia telah menggariskan hala tuju keselamatan melalui dokumen strategik seperti Kertas Putih Pertahanan 2019 dan Dasar Keselamatan Negara 2021–2025, pelaksanaan integrasi keselamatan masih belum mencapai tahap yang diperlukan untuk menghadapi ancaman rentas domain. Sistem-sistem keselamatan yang wujud beroperasi mengikut fungsi sektor masing-masing, mewujudkan ketidaksamaan aliran maklumat dan kebergantungan kepada prosedur koordinasi manual. Dalam persekitaran ancaman yang

bergerak laju, pendekatan berasaskan silo ini menyukarkan pembentukan gambaran operasi yang komprehensif serta memperlahankan keupayaan respon nasional.

Jadual 1 merumuskan dimensi utama ancaman hibrid yang memberi tekanan terhadap keselamatan negara, termasuk impak langsung terhadap keupayaan pemantauan maritim, keselamatan siber, kestabilan maklumat dan ketahanan kognitif. Implikasi pelbagai dimensi ini mengesahkan keperluan kepada rangka kerja keselamatan yang mampu menyatukan data serta risikan daripada pelbagai domain dalam satu struktur pengurusan yang lebih responsif.

**Jadual 1.** Evolusi ancaman hibrid dan implikasinya terhadap Malaysia

<b>Komponen ancaman</b>	<b>Ciri utama</b>	<b>Implikasi kepada Malaysia</b>	<b>Respons strategik atau tindakan C6ISR</b>
Fizikal dan maritim	Operasi kelabu, pencerobohan kapal asing, tekanan ketenteraan	Risiko kedaulatan di Laut China Selatan, keperluan pemantauan maritim berketepatan tinggi	Penggunaan pengawasan maritim bersepadu, integrasi sensor laut dalam C6ISR
Siber	Serangan siber, ransomware terhadap infrastruktur strategik	Ancaman kepada tenaga, telekomunikasi, perbankan dan keselamatan negara	Penyelarasan keselamatan siber nasional, integrasi perisikan siber dalam C6ISR
Maklumat	Disinformasi, propaganda digital, manipulasi media sosial	Polarisasi masyarakat, penghakisan kepercayaan terhadap institusi	Penubuhan unit respons maklumat, integrasi analitik maklumat dalam C6ISR
Ekonomi	Manipulasi geoekonomi, tekanan perdagangan	Gangguan rantaian bekalan dan risiko kebergantungan asing	Analisis ekonomi strategik dalam rangka C6ISR untuk sokongan keputusan
Kognitif	<i>Influence operations dan psychological shaping</i>	Menjejaskan perpaduan sosial dan ketahanan nasional	Pembangunan komponen kesedaran kognitif dalam C6ISR

Sumber: Hoffman, 2007; Alberts & Hayes, 2006; Joint Chiefs of Staff, 2018; Kementerian Pertahanan Malaysia, 2019; Majlis Keselamatan Negara, 2021

Berdasarkan jurang ini, kajian ini berhujah bahawa Malaysia memerlukan suatu kerangka C6ISR nasional yang dapat menghubungkan perintah, kawalan, komunikasi, persekitaran data, sistem tempur, keupayaan siber serta risikan multi domain dalam satu platform yang bersepadu. Model sedemikian bukan sahaja menyokong penghasilan gambaran operasi yang tepat, tetapi juga memperkukuh keupayaan membuat keputusan strategik secara masa nyata dalam menghadapi ancaman hibrid. Pengenalan ini seterusnya menyediakan asas kepada perbincangan mengenai justifikasi pembentukan Model C6ISR Nasional Malaysia, kerangka teori yang mendasari kajian serta keperluan untuk menilai amalan terbaik antarabangsa sebagai rujukan pembangunan sistem keselamatan negara yang lebih holistik dan bersepadu.

## Sorotan literatur

Sorotan literatur mengenai keselamatan nasional dan sistem perintah serta kawalan moden menunjukkan bahawa pengurusan ancaman hibrid memerlukan integrasi maklumat, kejelasan governans dan keupayaan operasi rentas domain. Berdasarkan penelitian terhadap karya teori, dasar keselamatan Malaysia dan pengalaman antarabangsa, literatur dapat dikelompokkan kepada tiga bidang utama: (i) asas konseptual dan teori keselamatan moden, (ii) jurang struktur keselamatan Malaysia dan (iii) amalan terbaik antarabangsa dalam pembangunan sistem C4I–C6ISR.

### *Asas konseptual dan teori keselamatan moden*

Perkembangan teknologi seperti kecerdasan buatan, pembelajaran mesin dan analitik data telah mengubah cara negara membina gambaran situasi dan membuat keputusan operasi. Dalam konteks ancaman hibrid, literatur menekankan bahawa keberkesanan sesuatu sistem keselamatan bergantung kepada tahap penyepaduan maklumat dan hubungan rentas domain.

Securitisatation Theory oleh Buzan, Wæver dan De Wilde (1998) menjelaskan bagaimana isu seperti pencerobohan maritim, serangan siber atau manipulasi maklumat dianggap ancaman keselamatan apabila dibingkaikan melalui wacana institusi. Pemahaman ini penting dalam konteks Malaysia kerana proses sekuritisasi mempengaruhi bagaimana negara mengatur semula keutamaan strategik dan keperluan integrasi sistem keselamatan.

Konsep Multi Domain Operations (Joint Chiefs of Staff, 2018) pula menegaskan bahawa ancaman moden berlaku secara serentak dalam pelbagai domain, justeru memerlukan penyelarasan data, sensor dan tindakan operasi dalam satu rangka kerja bersama. Keperluan ini diperkukuh oleh pendekatan Network Centric Warfare (Alberts & Hayes, 2006) yang memberi penekanan kepada kelebihan maklumat melalui perkongsian data masa nyata.

Dalam domain geospasial, GEOINT Fusion (National Geospatial-Intelligence Agency, 2021) memperkenalkan kepentingan menggabungkan imejan, radar, metadata lokasi dan risikan digital. Kajian terkini turut menunjukkan bahawa kecerdasan buatan meningkatkan ketepatan amaran awal dan pemprosesan maklumat merentas domain (Tuvdendarjaa, 2025; Romei de Socio et al., 2025).

Secara keseluruhan, literatur teori menunjukkan kesepakatan bahawa integrasi maklumat merupakan tunjang kepada keberkesanan sistem keselamatan moden. Namun keberkesanan ini hanya dapat dicapai melalui kerangka institusi dan infrastruktur data yang menyokong perkongsian maklumat secara holistik.

### *Jurang struktur keselamatan Malaysia*

Literatur kebangsaan, termasuk Dasar Keselamatan Negara 2021–2025 dan Kertas Putih Pertahanan 2019, menunjukkan bahawa ekosistem keselamatan Malaysia masih beroperasi berasaskan pendekatan sektoral dan bidang kuasa agensi yang terpisah. Pendekatan ini mewujudkan aliran data yang tidak seragam serta menyukarkan pembentukan gambaran operasi nasional yang menyeluruh dan bersepadu. Kajian oleh Mohammed Zain et al. (2023) mendapati bahawa tahap koordinasi perkongsian maklumat antara agensi keselamatan masih berada pada tahap yang rendah, sebahagiannya berpunca daripada ketiadaan standard teknikal bersama dan protokol interoperabiliti yang jelas. Kekangan struktur ini seterusnya menjejaskan keupayaan negara untuk menghasilkan *Common Operating Picture*, khususnya dalam situasi krisis yang memerlukan tindak balas pantas dan penyelarasan rentas agensi.

Literatur tempatan turut memperlihatkan bahawa kajian keselamatan di Malaysia cenderung memberi tumpuan kepada domain sektoral yang terasing, seperti keselamatan

maritim, keselamatan siber, pengurusan bencana atau komuniti pertahanan tertentu. Namun demikian, masih belum wujud kajian komprehensif yang menyatukan domain fizikal, digital dan kognitif dalam satu rangka keselamatan nasional yang bersepadu. Ketiadaan model integrasi nasional ini mencerminkan jurang akademik dan dasar yang signifikan, sekali gus mengesahkan keperluan untuk membangunkan satu kerangka C6ISR di peringkat negara.

*Pembelajaran antarabangsa dan amalan terbaik C4I–C6ISR*

Kajian menunjukkan bahawa negara yang berjaya mengurus ancaman hibrid mempunyai sistem perintah dan kawalan yang menyepadukan data, risikan dan operasi dalam satu ekosistem nasional. Walaupun model dan doktrin berbeza, kesemua negara mencapai satu ciri utama: integrasi komponen C1 hingga C6 dengan ISR dalam rangkaian data kebangsaan.

Amerika Syarikat sebagai contoh, mengembangkan Joint All-Domain Command and Control (JADC2) bagi memastikan integrasi sensor dan keupayaan tembakan secara masa nyata. Singapura pula menekankan integrasi awam-tentera melalui sistem Sense–Make–Act yang menghubungkan Singapore Armed Forces (SAF) dan Home Team. Korea Selatan memanfaatkan radar jarak jauh, kecerdasan buatan dan pertahanan siber sebagai sebahagian daripada C5ISR, manakala Turkiye membina ekosistem C6ISR berasaskan dron bagi menyepadukan sensor, platform tempur dan peperangan elektronik.

Jadual 2 menunjukkan perbandingan ringkas keempat-empat negara ini. Secara umum, kesemua negara menekankan: 1) integrasi maklumat dan *data fusion* sebagai asas ketepatan operasi, 2) penggunaan AI untuk mempercepatkan keputusan, dan 3) penyepaduan antara sistem tempur dan risikan. Walaupun konteks Malaysia berbeza, literatur antarabangsa memberikan gambaran bahawa keupayaan keselamatan nasional moden bergantung pada sistem integrasi berskala nasional yang menggabungkan fungsi perintah, kawalan, risikan, siber dan geospasial dalam satu ekosistem.

**Jadual 2.** Perbandingan model operasi dan amalan C6ISR antarabangsa dalam pengurusan ancaman hibrid

Negara	Model / Kerangka operasi	Komponen teras C6ISR	Ciri utama integrasi
Amerika Syarikat	Joint All-Domain Command and Control (JADC2)	C1–C6 + AI-enabled ISR	Integrasi satelit, radar, SIGINT, dron dan rangkaian siber; keupayaan <i>sensor-to-shooter</i> masa nyata; penggunaan AI untuk <i>decision superiority</i> dalam operasi multidomain
Singapura	National C4I System / Sense–Make–Act	C1–C4 + GEOINT + AI	Penyepaduan SAF-Home Team dalam satu rangkaian C4I nasional; analitik data untuk amaran awal; geospasial fusion sebagai asas pembentukan COP nasional. Model integrasi awam-tentera paling konsisten di Asia
Korea Selatan	AI-Driven C5ISR / ICT-Enabled Warfare	C1–C5 + radar + AI + siber	Integrasi radar darat-laut-udara dan sensor multidomain; penggunaan AI bagi analisis ancaman dan sistem amaran awal; struktur C2 yang selari dengan doktrin MDO untuk respons pantas terhadap ancaman Korea Utara

Turkiye	Türkiye C6ISR Ecosystem (Drone-Centric Architecture)	C1–C6 + Combat Systems + Cyber	Integrasi UAV MALE/HALE, radar AESA dan sistem tempur pelbagai domain; <i>data fusion</i> untuk operasi hibrid di Syria–Libya; dominan dalam peperangan elektronik, ISR taktikal dan operasi rentas domain
---------	--	--------------------------------	--

---

Sumber: Joint Chiefs of Staff, 2018; Raska, 2024; Seo, 2025; Oh et al., 2024; Sari & Bozkurt, 2025; Cantenar, 2023

### *Rumusan sorotan literatur*

Sorotan literatur menunjukkan bahawa ancaman hibrid hanya dapat ditangani melalui kerangka keselamatan bersepadu yang menyatukan maklumat, risikan dan operasi rentas domain. Literatur tempatan menegaskan bahawa Malaysia masih belum memiliki sistem sedemikian, manakala pengalaman antarabangsa membuktikan bahawa negara yang mengamalkan C5ISR atau C6ISR berada pada tahap kesiapsiagaan yang jauh lebih tinggi. Jurang akademik dan institusi ini memberikan asas yang kukuh bagi kajian ini untuk membangunkan Model C6ISR Nasional Malaysia sebagai rangka integrasi keselamatan multi domain.

## **Metodologi**

### *Reka bentuk kajian*

Kajian ini menggunakan reka bentuk kualitatif berasaskan analisis dokumen dan kajian konseptual, selaras dengan amalan penyelidikan dalam bidang keselamatan, dasar awam dan hubungan antarabangsa. Pendekatan ini dipilih kerana isu C6ISR dan keselamatan multi domain menuntut penilaian mendalam terhadap dasar negara, doktrin ketenteraan, laporan keselamatan serantau serta literatur akademik yang menerangkan konsep integrasi maklumat dan operasi rentas domain.

Menurut Creswell dan Creswell (2022), analisis kualitatif membolehkan penyelidik meneliti pola, makna dan interpretasi yang terkandung dalam dokumen strategik secara komprehensif. Pendekatan ini amat sesuai bagi kajian yang bertujuan membina model atau kerangka konseptual, khususnya apabila penyelidikan melibatkan penilaian struktur institusi keselamatan, jurang interoperabiliti serta keperluan transformasi sistem nasional.

### *Sumber data*

Kajian ini menggunakan dua kategori sumber data, iaitu sumber primer dan sumber sekunder. Pemilihan dibuat berdasarkan kredibiliti penerbit, akses terbuka, serta perkaitan langsung dengan objektif kajian.

#### a. Sumber primer

Sumber primer terdiri daripada dokumen rasmi kerajaan dan pertahanan yang mempunyai autoriti dalam pembentukan dasar keselamatan, GEOINT dan kerangka C4ISR–C6ISR. Dokumen tersebut ialah:

- Kertas Putih Pertahanan 2019, Kementerian Pertahanan Malaysia
- Dasar Keselamatan Negara 2021–2025, Majlis Keselamatan Negara

- Regional Security Outlook 2022, ISEAS–Yusof Ishak Institute
  - Joint All-Domain Command and Control (JADC2), Joint Chiefs of Staff (2018)
  - GEOINT Essential Body of Knowledge, National Geospatial-Intelligence Agency (2021)
- Dokumen ini dipilih kerana ia menyediakan asas rasmi bagi penilaian keupayaan keselamatan Malaysia dan piawaian antarabangsa dalam domain C4ISR–C6ISR.

#### b. Sumber sekunder

Sumber sekunder merangkumi artikel jurnal berindeks Scopus yang berkaitan dengan:

- C4ISR dan interoperabiliti sistem
- Multidomain Operations (MDO)
- Hybrid Warfare
- Geospatial Intelligence (GEOINT)
- Governans dan integrasi keselamatan

Sumber ini menyokong analisis teori dan memberikan asas empirikal untuk membandingkan amalan antarabangsa dengan konteks Malaysia.

#### *Proses analisis data*

Analisis data dijalankan menggunakan pendekatan analisis tematik, merangkumi tiga peringkat utama iaitu pengekodan awal, pembentukan tema, dan sintesis tematik.

#### a. Pengekodan awal

Setiap dokumen dianalisis untuk mengenal pasti konsep-konsep utama meliputi multidomain operations, risikan bersepadu, interoperabiliti C4I–C6ISR, ancaman hibrid, dan *data fusion*. Pengekodan awal ini membantu menghasilkan set konsep asas yang konsisten dengan objektif penyelidikan.

#### b. Pembentukan tema

Konsep-konsep yang telah dikodkan dikelompokkan kepada tema yang lebih besar. Antara tema utama ialah:

- Jurang struktur keselamatan Malaysia
- Keperluan pembangunan sistem C6ISR nasional
- Amalan terbaik dan model integrasi maklumat negara maju seperti Amerika Syarikat, Singapura, Korea Selatan dan Turkiye

Proses pengelompokan ini membolehkan pembinaan hubungan antara konsep dan memberi gambaran lebih jelas mengenai isu keselamatan multi domain Malaysia.

#### c. Sintesis tematik

Tema-tema utama digabungkan untuk membentuk kerangka awal Model C6ISR Nasional Malaysia. Proses ini selaras dengan panduan George dan Bennett (2005) yang menekankan peranan sintesis konsep dalam pembinaan teori dan model dalam penyelidikan keselamatan serta hubungan antarabangsa.

### *Kebolehpercayaan data*

Kebolehpercayaan kajian dipastikan melalui beberapa kaedah verifikasi termasuk triangulasi sumber, perbandingan silang dan pengesahan konsep.

#### *Triangulasi sumber*

Dapatan dibandingkan antara dokumen dasar Malaysia, laporan keselamatan serantau ISEAS dan literatur antarabangsa untuk meminimumkan bias analisis dan meningkatkan kesahan interpretasi.

#### a. Perbandingan silang

Kajian membandingkan Malaysia dengan empat negara rujukan yang mempunyai kematangan C4I–C6ISR yang lebih tinggi: Amerika Syarikat, Singapura, Korea Selatan dan Turkiye. Perbandingan silang ini membantu mengenal pasti elemen yang boleh diadaptasi serta jurang kritikal yang perlu ditangani oleh Malaysia.

#### b. Pengesahan konsep

Konsep utama seperti multidomain operations, GEOINT, *data fusion*, AI-enabled ISR dan command integration disahkan melalui doktrin rasmi (Joint Chiefs of Staff; National Geospatial-Intelligence Agency) dan rujukan akademik berwasit bagi memastikan ketepatan definisi dan aplikasi konsep dalam konteks keselamatan Malaysia.

**Jadual 3.** Ringkasan metodologi kajian

<b>Komponen</b>	<b>Perincian metodologi</b>
Reka bentuk	Kajian kualitatif berasaskan analisis dokumen dan kajian konseptual
Sumber primer	KPP 2019; DKN 2021–2025; ISEAS Regional Security Outlook 2022; JADC2 (Joint Chiefs of Staff, 2018); GEOINT EBK (NGA, 2021)
Sumber sekunder	Artikel Scopus berkaitan C4ISR, MDO, GEOINT, interoperabiliti dan hybrid warfare
Kaedah analisis	Analisis tematik: (i) pengekodan awal; (ii) pengelompokan tema; (iii) sintesis model
Rujukan metodologi	Creswell & Creswell (2022); George & Bennett (2005)
Kebolehpercayaan	Triangulasi sumber; perbandingan silang empat negara; pengesahan konsep

Sumber: Olahan penyelidik

### **Dapatan kajian**

Analisis dokumen dasar, laporan keselamatan serantau dan literatur akademik menunjukkan tiga pola utama yang menjelaskan kedudukan Malaysia dalam konteks keselamatan multi domain: (i) struktur keselamatan yang masih berasaskan silo institusi, (ii) integrasi C4I yang terhad, dan (iii) ketiadaan kerangka nasional yang menyatukan komponen C1–C6 dengan ISR.

Pola ini saling melengkapi serta membentuk rasional keperluan pembangunan Model C6ISR Nasional Malaysia.

*Struktur keselamatan Malaysia masih berasaskan silo institusi*

Analisis dokumen rasmi mendapati bahawa ekosistem keselamatan Malaysia melibatkan pelbagai agensi seperti MKN, ATM, PDRM, APMM, AKPS dan ESSCOM. Namun hubungan antara agensi ini kekal terpisah, khususnya dari segi perkongsian maklumat, interoperabiliti sistem perintah dan kawalan, serta penghasilan kesedaran situasi masa nyata. Dasar Keselamatan Negara 2021–2025 turut mengakui bahawa pengurusan keselamatan negara masih dipengaruhi oleh ketidaksejajaran aliran maklumat antara agensi, yang menjejaskan keupayaan menghasilkan gambaran strategik nasional yang holistik.

Ketiadaan suatu *National Security Operating Picture* menjadikan data maritim, udara, siber dan risikan taktikal tidak dapat digabungkan dalam platform bersama. Jadual 4 merumuskan jenis kekangan dalam struktur keselamatan serta implikasi strategiknya terhadap Malaysia. Kekangan ini memberi kesan ketara kepada operasi maritim, tindak balas siber, keselamatan sempadan dan pengurusan bencana. Dapatan ini mengesahkan bahawa isu keselamatan Malaysia bukan sahaja teknikal, tetapi melibatkan dimensi governans seperti yang turut disentuh dalam DKN 2021–2025.

**Jadual 4.** Kekangan struktur keselamatan Malaysia dan implikasi strategik nasional

Komponen	Kekangan	Implikasi strategik
Institusi	Fragmentasi ATM–PDRM–APMM–MKN	Tindakan tidak seragam, COP nasional lemah
Sistem C4I	Sistem tidak saling kendali	Keputusan lambat, operasi tidak selaras
Risikan	ISR tidak bersepadu	Maklumat kritikal tidak tiba masa nyata
Siber & data raya	Dipisahkan daripada C2	Kerentanan siber meningkat

Sumber: Olahan penyelidik

*Integrasi C4I Malaysia masih terhad dan tidak menyeluruh*

Kajian mendapati bahawa Malaysia masih bergantung kepada sistem *command and control* berbentuk C3/C4 sektoral, di mana data dan risikan tidak disepadukan antara sistem ketenteraan, keselamatan awam, operasi maritim dan pemantauan siber. Kertas Putih Pertahanan 2019 turut menegaskan keperluan transformasi C4I Malaysia, namun dokumen tersebut tidak merangka kerangka integrasi yang meliputi domain siber, geospasial dan kognitif secara nasional. Data pemantauan laut, radar udara, amaran awal siber dan maklumat risikan manusia kekal berada dalam silo institusi. Ketiadaan pusat *fusion* nasional menyukarkan pembentukan *common operating picture* yang diperlukan untuk operasi rentas domain.

*Ketiadaan model nasional yang menyatukan C1–C6 dengan ISR*

Perbandingan dokumen dasar ASEAN dan laporan keselamatan antarabangsa menunjukkan bahawa negara-negara seperti Amerika Syarikat, Turkiye, Singapura dan Korea Selatan telah melaksanakan sistem keselamatan multi domain melalui pusat C4I, C5ISR atau C6ISR. Malaysia, sebaliknya, belum membangunkan arkitektur C6ISR nasional, rangkaian data masa

nyata atau *ISR fusion centre*. Ketiadaan ini menghadkan integrasi antara domain maritim, udara, siber dan kognitif.

ISEAS Regional Security Outlook 2022 turut menekankan bahawa perubahan landskap keselamatan Indo-Pasifik menuntut setiap negara meningkatkan integrasi rentas domain, sesuatu yang belum wujud secara struktural dalam konteks Malaysia. Model C6ISR Nasional Malaysia yang dicadangkan dalam kajian ini bertujuan mengisi jurang kritikal ini untuk meningkatkan kesiapsiagaan strategik negara.

*Malaysia tertinggal berbanding negara yang lebih maju: Analisis perbandingan antarabangsa*

Analisis silang kes mendapati bahawa keempat-empat negara rujukan mempunyai model keselamatan multi domain yang dibina berasaskan integrasi data, risikan dan operasi. Sebagai contoh, JADC2 (Joint Chiefs of Staff, 2018) menunjukkan bagaimana penyepaduan lima domain dibangunkan melalui AI, data fabric dan integrasi sensor-to-shooter. Dalam perbandingan ini, Malaysia masih berada pada tahap C3/C4 sektoral.

**Jadual 5.** Perbandingan sistem C4I–C6ISR antarabangsa dan pengajaran untuk Malaysia

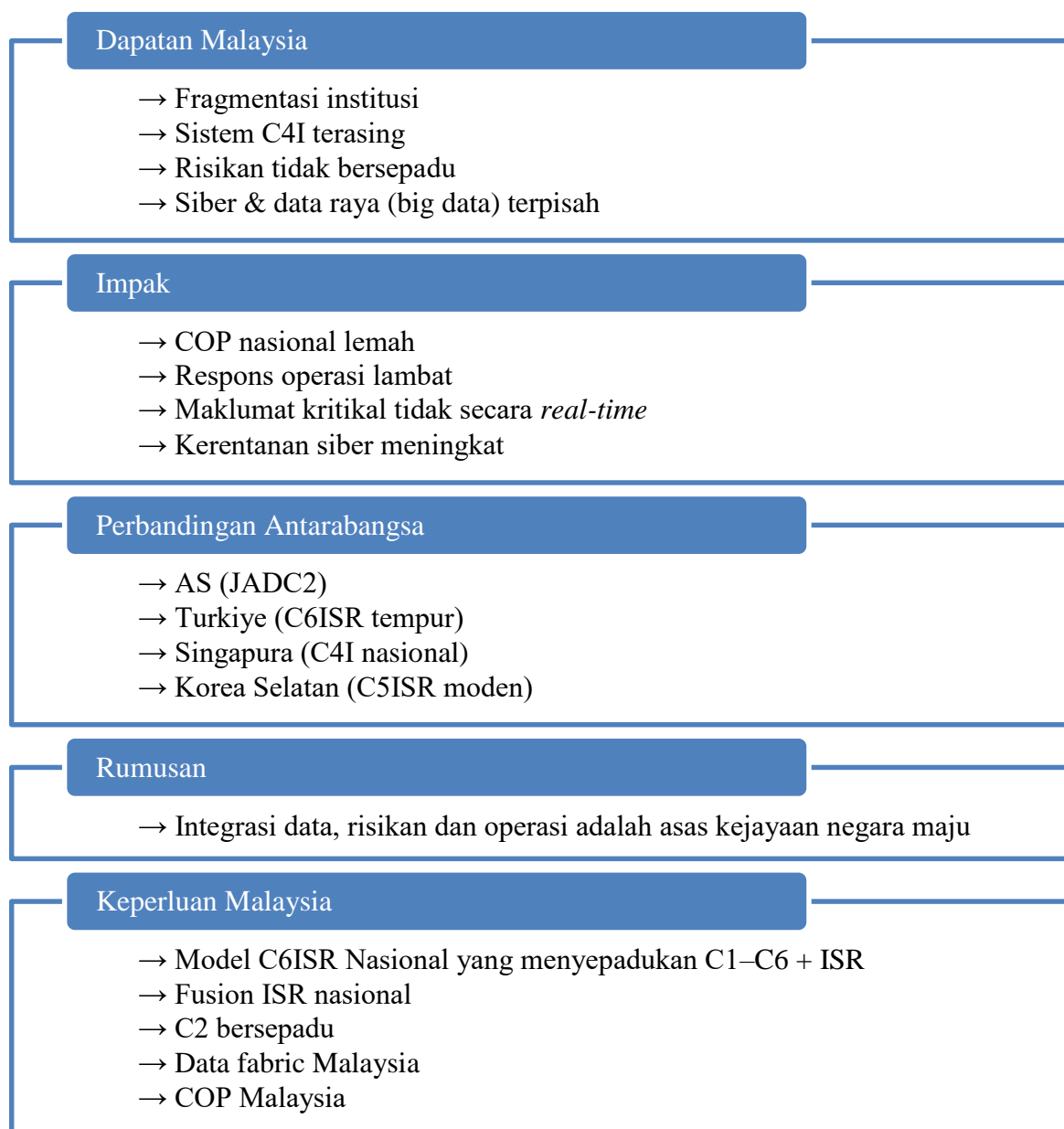
Negara	Tahap sistem	Keupayaan teras	Elemen C6ISR utama	Pengajaran kepada Malaysia
Amerika Syarikat	JADC2 (C6ISR penuh)	Integrasi lima domain, AI, cloud	COP global, data fabric	Pembinaan rangkaian data nasional masa nyata
Turkiye	C6ISR operasi	Dron MALE/HALE, radar AESA	Integrasi combat–ISR	Integrasi sistem tempur dan risikan
Singapura	C4I nasional	Sense–Make–Act	COP nasional	Keperluan pusat C6ISR negara
Korea Selatan	C5ISR moden	Radar, AI, siber	ISR multidomain	Integrasi radar–AI–siber
Malaysia	C3/C4 sektoral	Sistem terpisah	Tiada C6ISR	Tertinggal jauh

Sumber: Olahan penyelidikan

*Rumusan dapatan kajian*

Dapatan menunjukkan bahawa Malaysia masih berada pada tahap integrasi keselamatan yang terhad berbanding negara-negara yang telah menginstitusikan C4I–C6ISR nasional. Kekangan struktur institusi, ketidakserasian sistem C4I dan ketiadaan pusat fusion ISR menghalang pembentukan gambaran operasi nasional yang tepat. Perbandingan antarabangsa mengesahkan bahawa penyepaduan data, risikan dan operasi dalam satu ekosistem nasional merupakan ciri utama negara yang berjaya menangani ancaman hibrid. Maka pembangunan Model C6ISR Nasional Malaysia muncul sebagai keperluan strategik dan mendesak.

*Rajah konseptual: Arah aliran dapatan kajian dan keperluan C6ISR*



Sumber: Olahan penyelidik

**Rajah 1.** Rajah konseptual: Arah aliran dapatan kajian dan keperluan C6ISR

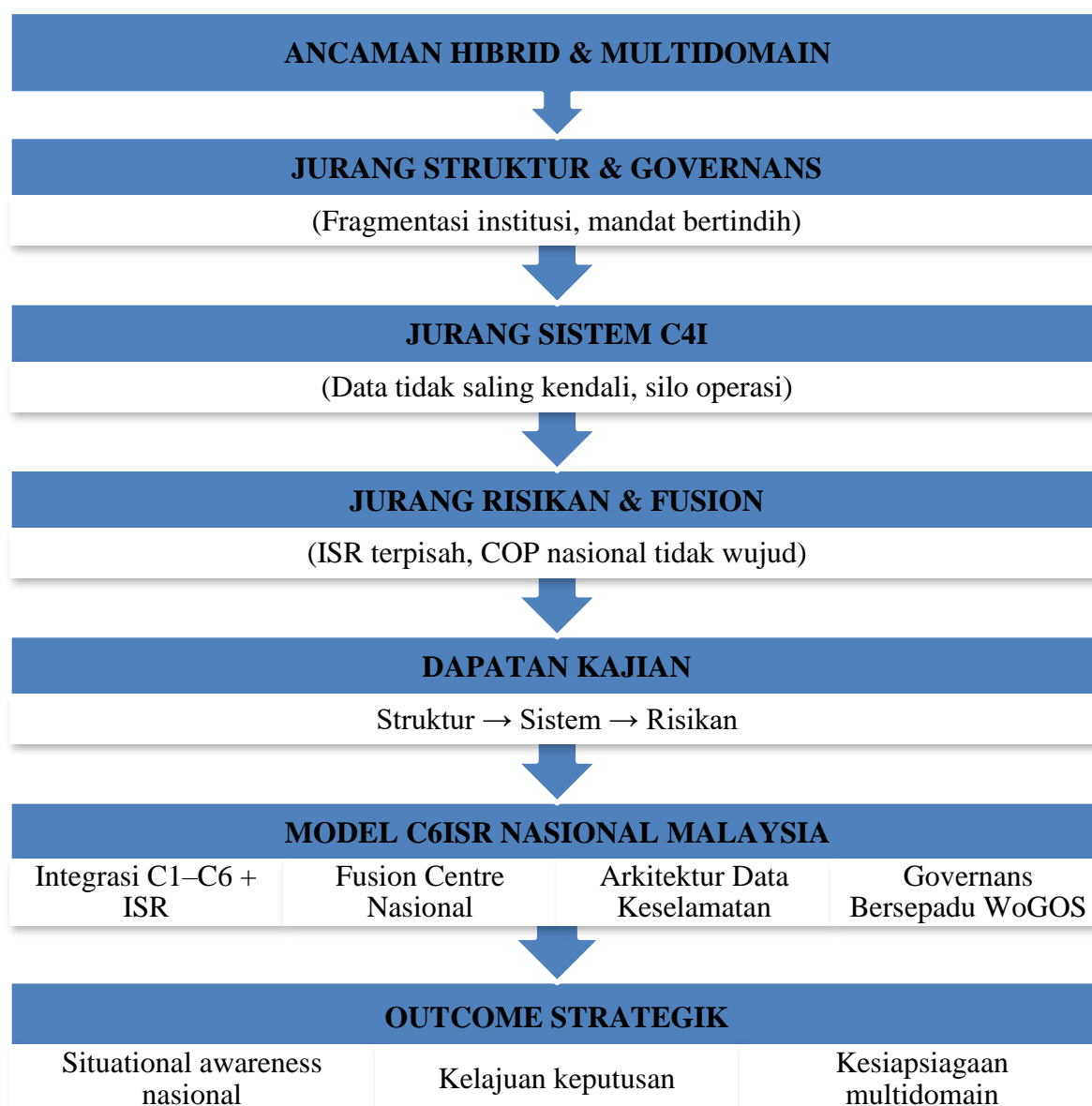
**Perbincangan**

Perbincangan ini menilai makna strategik dapatan kajian dan menjelaskan bagaimana kesemua pola yang ditemui menyokong keperluan pembentukan Model C6ISR Nasional Malaysia. Tumpuan diberikan kepada hubungan antara jurang struktur institusi, ketidakselarasan sistem C4I, ketiadaan keupayaan fusion ISR dan implikasi keselamatan multi domain. Perbincangan tidak mengulangi dapatan, tetapi menghuraikan mengapa jurang tersebut penting dan bagaimana ia menjejaskan keupayaan keselamatan negara.

### *Keperluan transformasi C6ISR dalam ekosistem ancaman multi domain*

Landskap keselamatan Malaysia kini dicirikan oleh ancaman fizikal, digital dan kognitif yang terjadi secara serentak. Dalam persekitaran seperti ini, maklumat tidak boleh terus berada di dalam silo organisasi. Kertas Putih Pertahanan 2019 menekankan keperluan memperkukuh C4I, tetapi dapatan menunjukkan bahawa Malaysia memerlukan transformasi yang lebih meluas sehingga merangkumi integrasi C1 hingga C6 serta risikan multi domain.

Pendekatan antarabangsa seperti JADC2 membuktikan bahawa ketepatan maklumat dan kelajuan keputusan hanya dapat dicapai apabila risikan, komunikasi, data, siber dan sistem tempur berada dalam satu rangka kerja yang disepadukan. Rajah 2 menggambarkan logik hubungan antara jurang struktur, jurang sistem dan keperluan membangunkan Model C6ISR Nasional.



Sumber: Olahan penyelidik

**Rajah 2.** Aliran logik pembentukan model C6ISR Nasional Malaysia

*Fragmentasi institusi dan keperluan penyelarasan governans keselamatan*

Antara penemuan paling signifikan kajian ialah kebergantungan Malaysia terhadap struktur institusi yang beroperasi secara terpisah. ATM, PDRM, APMM, ESSCOM dan MKN masing-masing mempunyai protokol, sistem data dan arkitektur maklumat tersendiri. Dasar Keselamatan Negara 2021–2025 turut mengakui bahawa ketidakseragaman aliran maklumat menjadi punca kepada kelambatan keputusan strategik. Perbincangan ini menegaskan bahawa pembentukan Model C6ISR Nasional bukan sekadar usaha teknikal, tetapi reformasi governans. Penyelarasan mandat keselamatan, penyeragaman standard interoperabiliti, dan kewujudan pusat fusion nasional merupakan syarat minimum untuk memastikan operasi rentas domain dapat dilaksanakan secara konsisten.

*Jurang teknologi C4I dan implikasi strategik terhadap operasi rentas domain*

Malaysia masih menggunakan sistem C3/C4 yang tidak disepadukan. Kekangan teknikal seperti ketiadaan *data fusion*, integrasi geospasial dan pemetaan multi domain menyebabkan gambaran operasi yang terhasil tidak menyeluruh. Dalam konteks ancaman kelabu dan disinformasi, kelewatan sedetik dalam kefahaman situasi boleh membawa implikasi strategik yang besar. Rujukan antarabangsa seperti NGA (2021) menunjukkan bahawa negara yang berjaya dalam operasi multidomain menggunakan integrasi risikan imejan, data siber, radar dan GEOINT dalam satu ekosistem. Jadual 6 berikut menempatkan kedudukan Malaysia berbanding negara rujukan, sekaligus menunjukkan jurang keupayaan operasi:

**Jadual 6.** Analisis perbandingan sistem C4I–C6ISR antarabangsa dan implikasi kepada Malaysia

Negara	Fokus sistem	Ciri utama	Kekuatan	Implikasi kepada Malaysia
AS	JADC2	AI, cloud, integrasi lima domain	Respons pantas, data fabric	Rangkaian data bersepadu diperlukan
Turkiye	C6ISR	UAV, radar AESA, systems-of-systems	Integrasi tempur–ISR	Integrasi ISR–geospasial negara
Singapura	C4I Nasional	Sense–Make–Act	Governans terpusat	Keperluan pusat fusion nasional
Korea Selatan	C5ISR	AI, radar, siber	ISR strategik	Pemantapan domain siber–geospasial
Malaysia	C3/C4	Silo institusi	Respons terhad	Pembinaan Model C6ISR Nasional

Sumber: Olahan penyelidik

*Pengajaran strategik daripada negara rujukan*

Analisis silang kes antarabangsa menunjukkan bahawa keberkesanan sistem keselamatan moden tidak lagi bergantung secara eksklusif kepada keunggulan teknologi, sebaliknya ditentukan oleh tahap integrasi institusi dan pengurusan maklumat yang bersepadu. Dapatan perbandingan ini memperlihatkan satu pola umum yang konsisten, iaitu gabungan integrasi governans dan integrasi data berfungsi sebagai pemangkin kepada kelebihan operasi merentas domain (*multidomain advantage*). Prinsip ini menjadi asas konseptual kepada pembentukan Model C6ISR Nasional yang dicadangkan untuk konteks Malaysia.

Dalam hal ini, Amerika Syarikat menonjol melalui penekanan terhadap kelajuan pemprosesan dan pengedaran maklumat sebagai faktor kritikal kelebihan operasi. Türkiye pula memperlihatkan pendekatan integratif yang menggabungkan keupayaan kenderaan udara tanpa pemandu (UAV), sistem radar dan platform tempur dalam satu ekosistem operasi bersepadu. Singapura memberi keutamaan kepada governans keselamatan yang terpusat bagi memastikan penyelarasan antara agensi dan keberkesanan pembuatan keputusan strategik. Sementara itu, Korea Selatan menumpukan pengukuhan keupayaan Intelligence, Surveillance and Reconnaissance (ISR) sebagai benteng utama dalam menjamin keselamatan negara.

### *Rumusan implikasi strategik kepada Malaysia*

Perbincangan perbandingan ini membawa kepada beberapa implikasi strategik yang signifikan terhadap landskap keselamatan negara Malaysia. Pertama, terdapat keperluan mendesak untuk mewujudkan satu kerangka penyepaduan nasional yang mampu menghubungkan domain darat, laut, udara, siber dan kognitif dalam satu gambaran strategik yang menyeluruh. Tanpa penyepaduan ini, keupayaan respons negara akan terus bersifat terpisah dan kurang berkesan. Kedua, reformasi governans keselamatan perlu dilihat sebagai prasyarat utama kepada transformasi sistem keselamatan negara. Struktur governans yang berpecah-pecah berpotensi melambatkan aliran maklumat dan melemahkan keupayaan membuat keputusan dalam situasi krisis. Ketiga, penubuhan sebuah pusat fusion nasional adalah penting bagi menyusun semula aliran data risikan, geospasial dan operasi secara sistematik dan bersepadu.

Akhirnya, pelaksanaan Model C6ISR Nasional berpotensi meningkatkan kelajuan pembuatan keputusan strategik serta memberikan kelebihan keputusan (*decision advantage*) kepada Malaysia, khususnya dalam menghadapi persekitaran keselamatan yang semakin kompleks dan dinamik. Pendekatan ini bukan sahaja memperkukuh kesiapsiagaan negara, malah menyokong pembentukan ekosistem keselamatan yang lebih adaptif dan berdaya tahan. Jadual 7 merumuskan jurang strategik Malaysia dan cadangan struktur C6ISR yang diperlukan.

**Jadual 7.** Jurang Strategik Malaysia dan Keperluan Pembentukan Model C6ISR

<b>Komponen</b>	<b>Jurang</b>	<b>Implikasi</b>	<b>Keperluan</b>
Governans Teknologi	Fragmentasi institusi Sistem tidak saling kendali	Arahan tidak seragam Masa keputusan lambat	Penyelarasan mandat Integrasi C1–C6
Risikan	ISR terpisah	Awareness rendah	Fusion Centre Nasional
Siber Operasi	Dipisahkan dari C2 Ketiadaan COP nasional	Kerentanan meningkat Respons tidak tepat	Integrasi siber–C2 COP Multidomain

Sumber: Olahan penyelidik

### **Kesimpulan**

Kajian ini menunjukkan bahawa Malaysia berdepan keperluan yang semakin penting untuk memperkukuh struktur keselamatan negara dalam menghadapi ancaman hibrid yang semakin kompleks dan merentas pelbagai domain. Berdasarkan analisis yang telah dibincangkan, cabaran utama yang dikenal pasti meliputi fragmentasi institusi, kewujudan sistem C4I yang tidak saling kendali, serta ketiadaan mekanisme fusion nasional yang benar-benar bersepadu. Keadaan ini memberi kesan kepada keupayaan negara untuk menyelaraskan maklumat, membina

kesedaran situasi bersama, dan merangka tindak balas yang lebih tersusun terhadap cabaran keselamatan semasa.

Dalam konteks tersebut, kajian ini mengemukakan suatu asas konseptual bagi Model C6ISR Nasional Malaysia yang menghimpunkan fungsi perintah, kawalan, komunikasi, data, sistem tempur, keselamatan siber dan risikan dalam satu kerangka yang lebih bersepadu. Cadangan ini tidak bertujuan menawarkan suatu model yang bersifat muktamad, sebaliknya sebagai kerangka awal untuk memahami keperluan penyelarasan yang lebih menyeluruh antara institusi, sistem dan proses dalam landskap keselamatan negara. Dengan itu, sumbangan utama kajian ini terletak pada usaha menghimpunkan dimensi teknikal, institusi dan governans dalam satu perbincangan yang lebih tersusun tentang keperluan transformasi keselamatan nasional.

Sehubungan itu, kajian lanjutan wajar dilaksanakan bagi meneliti dengan lebih mendalam aspek reka bentuk seni bina C6ISR, tahap kesiapsiagaan institusi, keperluan interoperabiliti data keselamatan, serta bentuk simulasi operasi multi domain yang sesuai dengan konteks Malaysia. Secara keseluruhan, kajian ini diharapkan dapat menjadi rujukan awal dalam memperkukuh perbahasan akademik dan dasar berhubung pembangunan sistem keselamatan negara yang lebih bersepadu, responsif dan sesuai dengan tuntutan persekitaran strategik semasa.

## Rujukan

- Alatas, S. M. (2016). The South China Sea and energy security: Malaysia's reaction to emerging geopolitical reconfigurations. *African and Asian Studies*, 15(1), 33–52.
- Alberts, D. S., & Hayes, R. E. (2006). *Understanding Command and Control*. CCRP Publication Series.
- Buzan, B., Wæver, O., & De Wilde, J. (1998). *Security: A New Framework for Analysis*. Lynne Rienner.
- Cantennar, Ö. F. (2023). *The rise of Turkey as a drone power: Implications for executive power enhancement* [Master's thesis, University College Dublin].
- Creswell, J. W., & Creswell, J. D. (2022). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (6<sup>th</sup> ed.). SAGE Publications.
- George, A. L., & Bennett, A. (2005). *Case Studies and Theory Development in the Social Sciences*. MIT Press.
- Hoffman, F. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies.
- Institute of Southeast Asian Studies. (2022). ISEAS regional security outlook 2022. ISEAS–Yusof Ishak Institute. <https://www.iseas.edu.sg/wp-content/uploads/2022/01/ISEAS-Regional-Security-Outlook-2022.pdf>
- Joint Chiefs of Staff. (2018). Joint all-domain command and control (JADC2): Concept overview. U.S. Department of Defense. [https://www.jcs.mil/Portals/36/Documents/Doctrine/Other\\_Pubs/jadc2\\_2018.pdf](https://www.jcs.mil/Portals/36/Documents/Doctrine/Other_Pubs/jadc2_2018.pdf)
- Kementerian Pertahanan Malaysia. (2019). Kertas Putih Pertahanan: Pertahanan Negara Semesta.
- Lai, Y. M., & Kuik, C. C. (2020). Structural sources of Malaysia's South China Sea policy: Power uncertainties and small-state hedging. *Australian Journal of International Affairs*, 75(3), 277–304.
- Majlis Keselamatan Negara. (2020). Malaysia Cyber Security Strategy 2020–2024.
- Majlis Keselamatan Negara. (2021). Dasar Keselamatan Negara 2021–2025.

- Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems*, 67, 6969–7055.
- Mohammed Zain, R., Mohd Zahari, H., & Mohd Zainol, N. A. (2023). Inter-agency information sharing coordination on humanitarian logistics support for urban disaster management in Kuala Lumpur. *Frontiers in Sustainable Cities*, 5, 1149454.
- National Geospatial-Intelligence Agency. (2021). GEOINT essential body of knowledge.
- Oh, S. J., Cho, S. K., & Seo, Y. (2024). Harnessing ICT-enabled warfare: A comprehensive review on South Korea's military meta power. *IEEE Access*, 12, 46379–46400.
- Rahim, S. S. I., Mohd Huda, M. I., Sa'ad, S., & Moorthy, R. (2024). Cyber security crisis/threat: Analysis of Malaysia National Security Council (NSC) involvement through the perceptions of government, private and people based on the 3P model. *e-Bangi Journal of Social Sciences & Humanities*, 21(2), 191–201.
- Rantos, K., Spyros, A., Papanikolaou, A., Kritsas, A., Ilioudis, C., & Katos, V. (2020). Interoperability challenges in the cybersecurity information sharing ecosystem. *Computers*, 9(1), 18.
- Raska, M. (2024). Reimagining Defense Innovation: Defense AI in Singapore. In H. Borchert, T. Schütz, & J. Verbovszky (Eds.), *The Very Long Game. Contributions to Security and Defence Studies*. Springer, Cham.
- Romei de Socio, M., Pozzato, G. L., & Merlo, A. (2025). A scalable ontology-driven architecture for situational awareness in multi-domain operations. *The Journal of Defense Modeling and Simulation Applications Methodology Technology*.
- Sari, K. A., & Bozkurt, M. E. (2025). Unmanned Aerial Vehicles (UAVs), the new actors of war: historical development, current situation and future. *Optimum Science Journal*.
- Seo, J. (2025). Strategic integration of artificial intelligence in the South Korean military: A framework for ethical, operational, and legal governance.
- Tuvdendarjaa, M.-O. (2025). Artificial intelligence in contemporary peacekeeping operations.