Jurnal Siber Multi Disiplin (JSMD)
E-ISSN: 2987-0380
P-ISSN: 2987-0402
+62 822 1012 3600 https://research.e-siber.org siberpublisher.info@gmail.com
DOI: https://doi.org/10.38035/jsmd.v4i3
https://creativecommons.org/licenses/by/4.0/

Diplomasi Pertahanan Australia Melalui AUKUS Dalam Transfer Teknologi Siber Untuk Menghadapi Ancaman Siber Tiongkok

Vanessya Meyva Latupeirissa[1], Indra Wisnu Wibisono[2], Roberto Octavianus Cornelis Seba[3].
[1]Universitas Kristen Satya Wacana, Salatiga, Indonesia, vanessyaltprssa16@gmail.com
[2]Universitas Kristen Satya Wacana, Salatiga, Indonesia, indra.wibisono@uksw.edu
[3]Universitas Kristen Satya Wacana, Salatiga, Indonesia, Roberto.seba@uksw.edu

Corresponding Author: vanessyaltprssa16@gmail.com[1]

Abstract: *Technological advancements in the era of globalization have expanded the scope of national security into cyberspace, which is now regarded as the fifth strategic domain in military operations. This study aims to analyze Australia's defence diplomacy through the AUKUS trilateral partnership, specifically under Pillar II in leveraging cyber technology transfer mechanisms to counter and respond to cyber threats posed by Tiongkok in the Indo-Pacific region. Tiongkok cyber threat driven by its ambition to become a cyber superpower and its military civil fusion strategy manifests through espionage operations, data theft, and attacks on critical infrastructure involving Advanced Persistens Threat (APT) groups affiliated with the Tiongkok military and intelligence agencies. Utilizing a qualitative descriptive-analytical approach, this research examines the interplay between national security concepts, cyber threats, cyber defence, technology transfer and defence diplomacy. The findings indicate that Australia utilizies AUKUS defence diplomacy via hybrid cyber technology transfer (combining vertical and horizontal methods) with the United Statesand the United Kingdom. The implementation includes joint military exercises (such as Exercise Talisman Sabre), testing of the Joint Cyber Hunt Kit, development of artificial intelligence, integration of autonomous systems, real time intelligence sharing and the deployment of advanced tooling to secure defence supply chains. This study concludes that cyber technology transfer involves not only the transfer of hardware and software but also the enhancement of human resource capacity, military interoperability, and the resilience of Australia's critical cyber infrastructure in responding to Tiongkok cyber threats in the region.*

Keyword: *AUKUS Pillar II, Cyber Defence, Cyber Technology Transfer, Defence Diplomacy, Tiongkok Cyber Threats.*

Abstrak: Perkembangan teknologi di era globalisasi telah memperluas cakupan keamanan nasional ke dalam dimensi ruang siber, yang kini dipandang sebagai domain strategis kelima dalam operasi militer. Penelitian ini bertujuan untuk menganalisis diplomasi pertahanan Australia melalui aliansi trilateral AUKUS, khususnya pada Pillar II dalam memanfaatkan mekanisme transfer teknologi siber untuk mengimbangi dan merespons ancaman siber dari Tiongkok di kawasan Indo-Pasifik. Ancaman siber Tiongkok yang didorong oleh ambisi

menjadi *cyber superpower* dan strategi penyatuan fusi militer-sipil diwujudkan melalui operasi spionase, pencurian data, serta serangan terhadap infrastruktur kritis yang melibatkan kelompok *Advanced Persistent Threat* yang berafiliasi dengan militer dan intelijen Tiongkok. Dengan menggunakan pendekatan kualitatif deskriptif analitis, penelitian ini mengkaji interaksi antara konsep keamanan nasional, ancaman siber, pertahanan siber, transfer teknologi dan diplomasi pertahanan. Hasil penelitian menunjukan bahwa Australia memanfaatkan diplomasi pertahanan AUKUS melalui transfer teknologi siber yang bersifat hibrida (gabungan vertikal dan horizontal) bersama Amerika Serikat dan Inggris. Bentuk implementasi transfer teknologi ini meliputi pelatihan bersama (seperti Latihan *Talisman Sabre*), pengujian *Joint Cyber Hunt Kit*, pengembangan kecerdasan buatan, integrasi sistem otonom, pertukaran data intelijen secara real-time hingga penggunaan *advanced tooling* untuk mengamankan rantai pasok pertahanan. Studi ini menyimpulkan bahwa transfer teknologi siber tidak hanya memindahkan perangkat keras dan lunak, melainkan juga meningkatkan kapasitas sumber daya manusia, interoperabilitas militer serta ketahanan infrastruktur siber kritis Austalia dalam merespons ancaman siber Tiongkok di kawasan.

Kata Kunci: Ancaman Siber Tiongkok, AUKUS Pillar II, Diplomasi Pertahanan, Transfer Teknologi Siber, Pertahanan Siber.

PENDAHULUAN

Perkembangan teknologi di era globalisasi menciptakan perubahan keamanan nasional yang mencakup ranah ruang siber (*cyberspace*). Dalam konteks pertahanan ruang siber menjadi domain strategis yang sama pentingnya dalam operasi militer selain darat, laut, udara, dan luar angkasa. Fenomena ini merupakan dampak dari perkembangan kegiatan siber yang dilakukan oleh manusia yang di satu sisi menunjukkan kemajuan peradaban teknologi namun di sisi lain telah menimbulkan ancaman yang semakin sulit untuk dikendalikan seperti ancaman siber yang menargetkan infrastruktur kritis seperti teknologi informasi dan telekomunikasi (jaringan, data sensitif, dan sistem komunikasi pemerintah/militer dll). Berkembangnya ancaman di ruang siber merupakan arus globalisasi karena adanya aktivitas teknologi informasi yang saling terhubung sehingga menimbulkan kekhawatiran para aktor negara. Menurut *International Telecommunication Union* dari laporan *Global Cybersecurity Index*, lebih dari 98% negara di dunia telah mengimplementasikan keamanan siber ke strategi pertahanan nasional mereka hal tersebut menunjukkan bahwa ancaman terhadap keamanan nasional tidak lagi terbatas pada serangan fisik atau operasi militer konvensional namun melibatkan ruang siber sebagai salah satu ruang strategis baru yang menghadirkan berbagai ancaman non-konvensional seperti ancaman siber (Darumaya, Maarif, Toruan, & Swastanto, 2023; ITU, 2024).

Ancaman siber merupakan efek globalisasi yang menjadi isu dalam setiap agenda keamanan nasional yang memicu kekhawatiran negara-negara untuk memperkuat kembali pertahanan siber untuk melindungi infrastruktur penting dan mengimbangi potensi serangan siber (Thekkekara, 2025). Kondisi ini memunculkan kekhawatiran Australia terhadap aktivitas siber dari Tiongkok karena Buku Putih Pertahanan dan Keamanan Tiongkok menunjukkan negara tersebut ingin mendominasi panggung global sebagai negara siber terbesar dibuktikan melalui kemandirian teknologi tingkat tinggi (*high-tech*) sebagai salah satu strategi Tiongkok dalam geopolitik global *(The People's Republic Of China*, 2019; Mo, 2025). Kemandirian *high-tech* Tiongkok ditopang oleh strategi nasional yang memadukan modernisasi militer dan sipil melalui kebijakan penyatuan fusi militer-sipil untuk menjadi *cyber superpower* (Brathwaite, 2025). Ambisi Tiongkok terbukti dalam dokumen pedoman keamanan siber yang diterbitkan oleh berbagai lembaga keamanan negara menyatakan Tiongkok merupakan aktor yang memanfaatkan ruang siber sebagai instrumen operasi pengumpulan informasi dan spionase terhadap berbagai negara dengan mensponsori kelompok siber untuk menargetkan jaringan di

seluruh dunia. Kelompok-kelompok tersebut seperti *Salt Typhoon*, Operator Panda dan RedMike, dll diistilahkan *Advanced Persistent Threat* (APT) dan terindikasi memiliki hubungan dengan perusahaan-perusahaan seperti *Sichuan Juxinhe Network Technology, Beijing Huanyu Tianqiong Information Technology, dan Sichuan Zhixin Ruijie Network Technology* untuk melakukan operasi peretasan hal ini tentunya mengancam keamanan siber Australia. Mereka terafiliasi dengan Tentara Pembebasan Rakyat (PLA) dan Kementerian Keamanan Negara Tiongkok yang dibuktikan melalui laporan *Annual Cyber Threat* Australia 2024-2025, bahwa kelompok APT 40 terindikasi melakukan ancaman pencurian data di bawah arahan Kementerian Keamanan Negara Tiongkok, merupakan lembaga yang bertanggung jawab atas pengumpulan intelijen asing untuk Tiongkok serta tiga perusahaan berbasis di Tiongkok yang bertugas menyediakan produk dan layanan siber kepada badan intelijen Tiongkok melalui operasi peretasan dari infrastruktur penting berbagai negara untuk digunakan dalam mengidentifikasi, melacak komunikasi dan pergerakan target di seluruh dunia (Australian, Governance, 2025; Australian, Governance, 2025).

Modernisasi militer dan aktivitas siber dari Tiongkok berkembang sampai ke Indo-Pasifik sebagai pusat persaingan strategis di abad ke-21, Australia melihat hal tersebut sebagai persaingan yang mampu mengancam *cyber domain* mereka meskipun kedua negara tersebut dipisahkan oleh bentangan maritim yang luas namun dalam ruang siber jarak fisik menjadi tidak relevan (Baram, 2025). Motif ancaman siber dari Tiongkok terhadap Australia karena persaingan kedua negara di kawasan, salah satu bentuk persaingan Australia-Tiongkok adalah persaingan keamanan di Indo-Pasifik yang menjadi pusat aktivitas geopolitik. Diketahui bahwa Tiongkok terus memperluas pengaruhnya di kawasan melalui modernisasi militer dan keterlibatan Tiongkok dengan *non state-sponsored* (APT) hal tersebut mengganggu *cyber domain* Australia sebagaimana tercantum dalam Strategi Pertahanan Nasional Australia bahwa Tiongkok terus meningkatkan kemampuan di semua bidang teknologi unggul dan telah meluncurkan senjata konvensional yang semakin maju serta mereka terus meningkatkan penelitian dan pengembangan teknologi, dimana selaras dengan Buku Putih Tiongkok untuk kemandirian teknologi tingkat tinggi (Australian Government, 2026; Siswoyo, 2025).

Dinamika ancaman siber yang mengancam keamanan nasional berdampak pada kekhawatiran Australia terhadap aktivitas ancaman siber dari Tiongkok yang disebabkan oleh persaingan di Indo-Pasifik maka terbentuklah AUKUS sebagai respons strategis terhadap kondisi keamanan kawasan. AUKUS adalah kemitraan keamanan trilateral antara Australia, Inggris dan Amerika Serikat yang diumumkan pada September 2021, berfokus pada berbagi teknologi transformasi yang berkontribusi untuk memperkuat kemampuan negara anggota mitra. AUKUS memiliki dua pilar yang mendasari pembentukan kemitraan ini yaitu, Pillar I berfokus pada kapal selam bertenaga nuklir untuk Australia dan Pillar II untuk pengembangan dan peningkatan kerja sama teknologi canggih antar angkatan bersenjata. Berdasarkan Strategi Pertahanan Nasional Australia tahun 2024, Pillar II mencakup enam bidang teknologi yaitu kemampuan bawah laut, kecerdasan buatan, sains kuantum, teknologi hipersonik, peperangan elektronik dan teknologi siber tingkat lanjut (Australian Government, 2024; Lubis, Perwita, & Hadisancoko, 2024). Mengingat aktivitas ancaman siber dari Tiongkok di Indo-Pasifik telah mengganggu *cyber domain* Australia, maka Pillar II AUKUS khususnya teknologi siber tingkat lanjut akan memberikan peningkatan pertahanan siber bagi Australia untuk melindungi infrastruktur kritis dan data sensitif dari ancaman siber Tiongkok dengan menggunakan instrumen transfer teknologi siber melalui diplomasi pertahanan (Siswoyo, 2025).

Transfer teknologi digunakan sebagai instrumen diplomasi pertahanan Australia dengan AUKUS (Amerika Serikat dan Inggris) melalui transfer pengetahuan, pelatihan dan pengembangan bersama untuk teknologi siber yang berimplikasi terhadap penguatan pertahanan dan keamanan siber Australia. Kemitraan ini memungkinkan adanya kolaborasi dan kesinambungan dalam pengujian, pelatihan dan operasi pelacakan siber di seluruh pasukan ketiga negara mitra serta memberikan kesempatan bagi *Australian Defence Force* (ADF) untuk

membawa pelajaran dari pelatihan yang diberikan AS dan Inggris untuk diterapkan di komando demi meningkatkan interoperabilitas ADF (Departmen Of War Innovation Unit, n.d.; Australian Government, 2024). Dari penguatan kemampuan ini, Australia bisa mengawasi pergerakan aktor maupun *non state-sponsored*, terutama dari ancaman siber yang berasal dari Tiongkok dan APT.

Mekanisme diplomasi pertahanan Australia melalui AUKUS dalam menghadapi ancaman siber dari Tiongkok merupakan model kerja sama dalam bentuk pengembangan berbagai kemampuan canggih, salah satunya adalah transfer teknologi siber untuk penguatan keamanan dan pertahanan siber dalam sistem komunikasi dan operasional kritis negara anggota, salah satunya Australia untuk melindungi diri dari ancaman Tiongkok. Transfer teknologi siber dalam kerangka Pillar II AUKUS berkontribusi pada peningkatan kapabilitas keamanan dan pertahanan siber Australia, dan berimplikasi terhadap diplomasi pertahanan serta penguatan siber Australia dalam merespons dinamika ancaman siber Tiongkok di Indo-Pasifik sebagai tantangan strategis dalam laporan *Annual Cyber Threat Australia* (Siswoyo, 2025).

Penelitian ini tidak sekedar memperluas landasan teoritik yang berfokus pada studi diplomasi dan siber namun menjelaskan bagaimana transfer teknologi menjadi penghubung antara diplomasi pertahanan dan ancaman siber yang membutuhkan respons cepat, akurat, dan ketahanan yang dinamis. ***Research gap*** penelitian berperan penting sebagai dasar konseptual untuk memahami sejauh mana peran diplomasi pertahanan Australia melalui AUKUS Pillar II dalam transfer teknologi siber untuk merespons ancaman siber Tiongkok. Joshi et al (2025) menjelaskan batasan keamanan nasional dan keamanan siber yang semakin kabur di era globalisasi; Wibisono et al (2019) meningkatkan kepentingan nasional Indonesia dalam ToT untuk kemandirian industri pertahanan dan bentuk diplomasi pertahanan dalam mencapai kesepahaman kerja sama dengan Turki; Lubis et al (2024) mengeksplorasi keberhasilan AUKUS dalam mengatasi tantangan yang dihadapi militer Australia sebelum bergabung dan dampak kerangka kerja AUKUS dalam meningkatkan kemampuan militer Australia; Effendy (2025) melihat bagaimana strategi perang siber China serta implikasi dominasi teknologi terhadap stabilitas keamanan regional; Putri et al (2022) menegaskan bahwa serangan *hacking tools predator* dapat mengancam keamanan siber dalam konteks sistem pertahanan negara. Secara keseluruhan, penelitian tersebut menyimpulkan bahwa implikasi teoritisnya terletak pada keamanan nasional dalam konteks kerja sama pertahanan melalui kerja sama AUKUS sebagai instrumen strategis untuk memperkuat kapabilitas pertahanan Australia dan memperluas kajian diplomasi pertahanan sebagai instrumen strategis dalam menghadapi ancaman non-konvensional dengan menelaah keterkaitan antara konsep ancaman siber, pertahanan siber, diplomasi pertahanan dan transfer teknologi dalam dinamika pertahanan.

METODE

Penulis menggunakan metode kualitatif dengan pendekatan deskriptif analitis. Menurut Given (2008), penelitian kualitatif adalah penelitian yang mengeksplorasi fenomena dengan mengungkapkan pikiran, perasaan, atau interpretasi orang atau individu dengan menekankan pada makna dan proses (Given, 2008). Pendekatan kualitatif digunakan untuk memahami secara mendalam dinamika diplomasi pertahanan Australia melalui AUKUS Pillar II, dalam konteks transfer teknologi siber untuk menghadapi ancaman siber Tiongkok. Penelitian kualitatif membantu penulis untuk mengamati serta memahami kerja sama diplomasi pertahanan dalam transfer teknologi siber dalam konteks praktis maupun normatif.

Pengumpulan data penelitian digunakan untuk mengumpulkan informasi yang diperlukan dalam penelitian. Penelitian ini menggunakan metode telaah pustaka dengan mengkaji berbagai sumber sekunder yang relevan, seperti buku, artikel jurnal ilmiah, laporan resmi lembaga pemerintah, serta dokumen kebijakan yang berkaitan dengan topik penelitian, untuk memperoleh data, informasi dan analisis yang mendukung pembahasan penelitian secara

komprehensif. Pemilihan teknik pengumpulan data sangat penting karena dapat memengaruhi validitas dan reliabilitas hasil penelitian yang harus disesuaikan dengan tujuan penelitian, jenis data yang dibutuhkan, sumber data yang tersedia dan pertimbangan etis. Kombinasi beberapa teknik pengumpulan data juga sering digunakan untuk mendapatkan pemahaman yang lebih lengkap tentang masalah penelitian. Sumber data dalam penelitian ini adalah data sekunder dan teknik analisis yang digunakan dalam penelitian ini adalah analisis kualitatif deskriptif. Teknik analisis ini adalah mengolah dan menafsirkan data yang diperoleh dari berbagai sumber pustaka seperti buku, jurnal ilmiah, laporan resmi, serta dokumen kebijakan yang relevan dengan topik penelitian kemudian data tersebut diklasifikasikan, dibandingkan dan dianalisis secara sistematis untuk mengidentifikasi pola, hubungan serta makna yang berkaitan dengan fokus penelitian (Zainuddin & Wardhana, 2024).

HASIL DAN PEMBAHASAN

Cyber Domain Sebagai Ruang Ancaman Strategis Terhadap Keamanan Nasional Australia

Cyber domain sebagai domain operasional buatan manusia dalam *cyberspace* terdiri dari jaringan infrastruktur teknologi informasi, perangkat lunak, perangkat komputer, jaringan data dan interaksi manusia yang saling terhubung dan bergantung satu sama lain. Sebagai domain kelima dalam operasi militer, *cyber domain* berkembang menjadi ranah strategis bagi kebijakan aktor maupun *non-state* sebagai tempat untuk memproyeksikan kekuatan karena prinsip operasionalnya unik serta sifatnya yang diperebutkan menciptakan kerentanan dan kompleksitas dalam *cyber domain* memunculkan ancaman yang menempatkan berbagai aktor maupun *non-state* di bawah kendali ancaman siber sehingga *cyber domain* menjadi tempat ancaman non-konvensional terhadap keamanan dan pertahanan nasional sebuah negara. Para aktor maupun *non-state* yang melakukan ancaman siber seperti spionase dan sabotase terhadap infrastruktur kritis (jaringan, sistem, data dll) hingga *information warfare* dari jarak jauh yang secara anonim menempatkan *cyber domain* sebagai posisi sentral dalam kekuatan besar kontemporer. Pada akhirnya, perkembangan ini menuntut kemajuan yang setara dalam memahami ancaman di dalam *cyber domain* (Brathwaite, 2025; Siroli, 2018).

Ancaman siber menurut Putri et al merupakan ancaman yang memiliki potensi kejahatan dan berhubungan dengan teknologi informasi seperti perangkat keras maupun perangkat lunak sedangkan menurut Darumaya et al ancaman siber merupakan segala aktivitas yang menargetkan perangkat, jaringan, misi maupun infrastruktur penting yang menyebabkan kerugian karena mengancam kerahasiaan, integritas dan ketersediaan sistem dan informasi dalam hal ini perkembangan ancaman siber semakin pesat dan telah mencakup kehidupan dan kepentingan salah satunya kepentingan pertahanan. McDonnell dan Sayers mengkategorikan ancaman siber ke dalam tiga kelompok meliputi: ancaman siber perangkat keras dan lunak melalui kasus ancaman berdasarkan laporan *annual cyber threat* 2024-2025 yang terdeteksi oleh ACSC, ASD dan mitra internasional melaporkan keterlibatan Tiongkok dengan kelompok siber yang mengancam *router* dan perangkat *Internet of Things* (IoT) dalam operasi botnet yang menargetkan ribuan perangkat yang terhubung ke internet untuk membuat jaringan (botnet) yang akan digunakan dalam aktivitas siber. Botnet terdiri atas 260.000 perangkat termasuk di Australia yang digunakan peretas sebagai perantara untuk menyembunyikan identitas saat melancarkan serangan DDoS terhadap infrastruktur kritis dan sistem pemerintahan. Ancaman pencurian data dan informasi saat kelompok peretas APT 40 terindikasi melakukan pencurian data dan informasi di bawah arahan *Ministry of State Security* (MSS) Tiongkok untuk mengumpulkan intelijen asing dengan tujuan membobol jaringan kritis pemerintah maupun swasta Australia untuk memenuhi kepentingan Tiongkok serta memanfaatkan kerentanan *router* kecil (SOHO) untuk menyusup sehingga menimbulkan ancaman bagi Australia (Australian, Governance, 2025).

Berdasarkan Buku Putih Pertahanan dan Keamanan Tiongkok menunjukkan negara tersebut ingin mendominasi panggung global sebagai negara siber terbesar dengan mempercepat kemandirian teknologi tingkat tinggi (*high-tech*) mencakup pengembangan chip canggih, perangkat lunak industri, kecerdasan buatan (AI) dan teknologi kuantum. Pengembangan tersebut merupakan bagian dari strategi Tiongkok untuk memperkuat posisinya dalam geopolitik global melalui modernisasi nasional dan kemandirian Tiongkok dalam *high-tech* yang menjadikan *Cyber domain* sebagai instrumen bagi Tiongkok untuk memperoleh keunggulan strategis tanpa harus terlibat dalam konflik konvensional, terbukti Tiongkok menduduki posisi kedua secara global dalam *cyber domain* berdasarkan *cyber capabilities data* untuk memperoleh *power* dengan mengakses informasi penting, melemahkan infrastruktur lawan dan membentuk *information warfare* melalui pemanfaatan data dan informasi yang telah diperoleh sebelumnya untuk melakukan propaganda digital dengan tujuan melemahkan legitimasi yang mampu membangun narasi menguntungkan bagi kepentingan Tiongkok (Effendy, 2025; Cyber Capabilities Data, 2025).

Ambisi Tiongkok menjadi *cyber superpower* ditopang oleh strategi nasional yang memadukan modernisasi militer, kemajuan sektor sipil dan kapasitas kendali informasi melalui kebijakan penyatuan fusi militer-sipil melalui keterlibatan sektor swasta, akademisi dan aktor non-negara dalam mendukung pengembangan kapasitas siber nasional Tiongkok hal tersebut terbukti dengan perusahaan teknologi seperti Huawei dan ZTE *Corporation* beroperasi sebagai entitas bisnis dan memiliki hubungan dengan agenda siber PKT yang menyebabkan batas antara kepentingan sipil dan militer dalam pengembangan teknologi siber Tiongkok semakin kabur (Brathwaite, 2025). Disisi lain, Kementerian Keamanan Negara Tiongkok dan Tentara Pembebasan Rakyat (PLA) memanfaatkan jaringan global industri teknologi Tiongkok untuk mendukung aktivitas siber seperti spionase dan sabotase digital dibuktikan berdasarkan dokumen panduan keamanan yang diterbitkan oleh berbagai lembaga negara dan mereka diatur dalam kerangka hukum yang mewajibkan perusahaan dan individu untuk patuh pada kepentingan intelijen Tiongkok berdasarkan Undang-Undang Keamanan Siber tahun 2017, secara institusional memberi wewenang kepada Tiongkok untuk menyelipkan dan mengeksploitasi celah keamanan pada produk teknologi buatan Tiongkok yang mana berdampak pada produk teknologi yang beredar di luar negeri berpotensi membawa risiko keamanan seperti penyisipan pintu belakang (*backdoor*) dan eksploitasi kerentanan tersembunyi sehingga menjadikan rantai pasok teknologi Tiongkok sebagai instrumen potensial bagi operasi siber negara (Dohr, 2025).

Kepentingan keamanan nasional Tiongkok untuk mempercepat *high-tech* berdampak pada pertahanan nasional Australia yang mempengaruhi keamanan nasionalnya karena adanya dukungan dari fusi militer-sipil, Undang-Undang keamanan siber dan campur tangan *non-state actor* yang mengancam pertahanan dan keamanan siber Australia. Berdasarkan kasus-kasus ancaman siber dari Tiogkok kepada Australia menyebabkan *cyber domain* Australia berada di posisi tinggi akibat spionase dan keterlibatan asing yang mengancam kedaulatan nasional mereka dimana Australia menduduki peringkat kelima secara *global* dalam *cyber domain* dibandingkan Tiongkok yang berada di posisi kedua (Australian Government, 2026; Cyber Capabilities Data, 2025). Laporan *Annual cyber threat* 2024-2025 berdasarkan ASD dan ASCS mencatat lonjakan ancaman siber meliputi lebih dari 42.500 panggilan hotline (naik 16%), merespons lebih dari 1.200 insiden keamanan siber (naik 11%), serta melakukan lebih dari 1.700 notifikasi aktivitas siber kepada masyarakat terdampak (naik 83%) (Australian, Governance, 2025). Dengan demikian berdasarkan laporan tersebut, kelompok APT yang berafiliasi dengan Tiongkok terus menargetkan jaringan pemerintah, militer dan infrastruktur kritis Australia untuk spionase dan mengganggu jaringan Australia meskipun negara ini berusaha memberikan keamanan siber yang Australia miliki namun hal tersebut tidak menutup kemungkinan melindungi mereka dari ancaman siber Tiongkok dengan kapabilitas teknologi siber Tiongkok yang semakin unggul, karena itu kemampuan dan kapabilitas siber memiliki

peran penting bagi Australia untuk mengantisipasi ancaman siber dari Tiongkok dan APT yang menggangu *cyber domain* Australia.

Ancaman Siber Dari Tiongkok Dan Strategi Pertahanan Siber Australia

Menurut Galinec et al, pertahanan siber menekankan pada mekanisme dalam pertahanan jaringan komputer yang berfokus pada pemberian pencegahan, mendeteksi dan pemberian respons terhadap ancaman siber yang meningkatkan jumlah dan tingkat kecanggihan ancaman, mengharuskan sistem pertahanan siber menjadi kebutuhan krusial bagi setiap aktor negara (Galinec, Moznik, & Guberina, 2018). Berdasarkan Buku Putih Pertahanan dan Keamanan Tiongkok terkait kepentingan mereka untuk mendominasi panggung global sebagai negara siber terbesar melalui kemandirian teknologi tingkat tinggi dimana salah satu strategi Tiongkok untuk memperkuat posisi dalam geopolitik global yang didukung modernisasi fusi militer-sipil ternyata menimbulkan persaingan di Indo-Pasifik sebagaimana diketahui Tiongkok melakukan operasi peretasan terhadap berbagai negara di Indo-Pasifik dengan memanfaatkan *cyber domain* untuk melancarkan aksinya yang disponsori kelompok APT seperti pencurian data strategis, sabotase infrasrtuktur serta pengumpulan informasi intelijen untuk dikirimkan kepada PLA dan Kementerian Keamanan Negara Tiongkok (Effendy, 2025). Aksi tersebut dibuktikan melalui ancaman siber dari Tiongkok kepada Australia di Indo-Pasifik berdasarkan beberapa kasus ancaman yang dipublikasikan melalui laporan *Annual Cyber Threat* 2024-2025, dokumen pedoman keamanan siber dan kasus lainnya yang menimbulkan persaingan keamanan di Indo-Pasifik antara kedua negara.

Merespons aktivitas ancaman siber dan ambisi Tiongkok sebagai *cyber superpower*, yang membuat Australia khawatir akan kepentingannya maka dari itu Australia membentuk Strategi Pertahanan Nasional untuk mencegah segala tindakan yang memicu konflik maupun aktivitas ancaman siber terhadap Australia. Strategi Pertahanan Nasional Australia mengadopsi strategi penolakan yang bertujuan untuk mencegah konflik dan menangkal segala aktivitas ancaman serta menjadi panduan kontribusi pertahanan untuk pertahanan nasional yang meliputi semua domain operasional militer (laut, udara, darat, luar angkasa dan siber) adanya strategi penolakan mampu untuk mencegah Tiongkok dan APT mengambil tindakan yang merugikan kepentingan Australia di Indo-Pasifik dengan menunjukan kemampuan, kapabilitas dan tekad ADF yang kredibel melalui keterlibatan kerjasama dengan mitra internasional untuk berkontribusi pada stabilitas keamanan Indo-Pasifik dan memperkuat pencegahan terhadap ancaman dan konflik. Strategi Pertahanan Nasional 2026 melanjutkan arah strategi 2024 untuk meningkatkan pencegahan kolektif melalui kerjasama dengan sekutu dan mitra internasional untuk menunjukkan kapabilitas kolektif sebagai cara yang efektif dalam berkontribusi pada stabilitas keamanan Indo-Pasifik dan memperkuat pencegahan terhadap ancaman dalam hal ini ancaman siber dari Tiongkok terhadap pertahanan siber Australia di Indo-Pasifik (Australian Government, 2026).

Berdasarkan Strategi Pertahanan Nasional 2026 Australia menjelaskan tiga tujuan pertahanan strategis meliputi: Mencegah tindakan seperti ancaman dan konflik yang merugikan kepentingan Australia melalui mitra internasional untuk memperkuat kemampuan individu melalui pembentukan AUKUS untuk peningkatan kapabilitas pertahanan trilateral, inovasi dan teknologi yang memungkinkan Pillar II AUKUS memperkuat kapabilitas pertahanan siber Australia terhadap ancaman siber dari Tiongkok melalui transfer teknologi siber sebagai instrumen dalam diplomasi pertahanan. Kemampuan untuk mencegah, mendeteksi dan merespons ancaman siber dari Tiongkok sangat penting bagi pertahanan siber Australia karena itu AUKUS meningkatkan kemampuan siber tingkat lanjut dengan menyediakan alat dan teknologi siber yang dibutuhkan untuk melawan ancaman Tiongkok melalui pengembangan dan integrasi teknologi deteksi dan merespons ancaman tingkat lanjut melalui sebuah sistem yang dapat meningkatkan kemampuan mitra AUKUS (Australia) untuk mengidentifikasi dan menetralisir ancaman siber secara *real-time*, berbagi intelijen AUKUS, melindungi aset dan

informasi penting melalui infrastruktur siber yang kuat agar mampu menahan dan pulih dari ancaman siber yang mana hal tersebut sangat perlu diperhatikan untuk menjaga kesinambungan operasional sistem dan layanan kritis (AUKUS Forum, 2024).

Dengan mencegah ancaman siber dari Tiongkok yang mengganggu *cyber domain* Australia dengan membentuk kerja sama AUKUS lewat transfer teknologi sebagai instrumen yang mana hal ini akan, membentuk lingkungan strategis Australia dengan mitra internasional melalui upaya Australia untuk menjaga perdamaian, kemakmuran, konflik dan ancaman salah satunya melalui keterlibatan ADF dan mitra internasional AUKUS di Indo-Pasifik seperti pelatihan, penelitian dan pengembangan bersama untuk teknologi siber yang dapat memberikan kapabilitas pertahanan siber bagi ADF dalam mendukung strategi penolakan melalui jaringan intelijen, dan sistem komando canggih dapat memberikan ADF dalam merespons setiap ancaman dengan cepat dan tepat yang akan menjadi daya gentar untuk menolak dan menggagalkan aktivitas siber (Australian Government, 2026).

Diplomasi Pertahanan Australia Melalui AUKUS Pillar II

Diplomasi pertahanan menurut Andrew Cottey dan Anthony Foster adalah diplomasi pertahanan yang menggunakan kekuatan militer dan infrastruktur secara damai khususnya peran Kementerian Pertahanan sebagai alat dari kebijakan luar negeri dan keamanan negara (Wibisono, Mahroza, & Poespitohadi, 2019). Pendekatan tersebut memperluas maknanya dengan mempertimbangkan penggunaan angkatan bersenjata secara damai, peran Kementerian Pertahanan dan penggunaan atase pertahanan untuk mencegah konflik. Kerja sama pertahanan trilateral yang dilakukan oleh Australia, Amerika Serikat dan Inggris merupakan salah satu dari proses diplomasi pertahanan yang dilakukan oleh Australia. AUKUS dikatakan sebagai diplomasi pertahanan karena dalam prosesnya terdapat aktivitas diplomasi pertahanan seperti yang disampaikan oleh Cottey dan Foster untuk menjaga ketahanan dan pencapaian Pillar II. Dalam proses kerja sama, negara anggota AUKUS telah memenuhi beberapa aktivitas diplomasi pertahanan menurut Cottey dan Foster, yaitu: 1) *Bilateral defence cooperation agreements*; 2) *Training of foreign military and civilian defence personnel*; 3) *Provision of military equipment and other material aid* (Cottey & Forster, 2004).

Berdasarkan *bilateral defence cooperation agreements*, hubungan trilateral ketiga negara dibentuk dalam sebuah kesepakatan pertahanan antara Australia, Inggris dan Amerika Serikat pada 15 September 2021 sebagai kemitraan berbagi teknologi dan kemampuan inovasi melalui Pillar I yaitu pengadaan kapal selam bertenaga nuklir yang dipersenjatai secara konvensional untuk Australia sedangkan Pillar II akan melakukan kerja sama dalam berbagai kemampuan keamanan dan pertahanan di mana setiap negara mitra akan memiliki kemampuan yang dibutuhkan untuk bertahan melawan ancaman yang semakin berkembang (Australian Government, 2023). Pillar II sama pentingnya dengan Pillar I karena akan memberikan pengembangan dan penyampaian kemampuan tingkat lanjut bagi negara anggota yang mana secara kolektif akan membuat militer AUKUS mampu beroperasi bersama sebagai satu kemitraan gabungan kekuatan dan akan menjadi lebih kuat serta menjadi daya gentar bagi Tiongkok. Mereka akan berkolaborasi secara mendalam dengan seluruh industri pertahanan trilateral di sisi lain secara individu para mitra akan lebih tangguh karena mendapatkan akses teknologi mutakhir yang sulit untuk mereka kembangkan secara mandiri karena itu bagi Australia hal ini mendukung Strategi Pertahanan Nasional dan Program Investasi Terpadu tahun 2026 untuk memperkuat kapasitas pertahanan mereka dalam melindungi dan mempertahankan negara serta kepentingan di tengah ketidakpastian global yang semakin mengancam dan sulit diprediksi (Australian Government, n.d.). Diplomasi Pertahanan Australia melalui AUKUS dapat meningkatkan kerja sama pertahanan siber yang termuat dalam Pillar II lewat penggabungan dan pembagian data yang cepat dalam operasi multi domain agar Australia bertindak lebih cepat dan tepat dalam menghadapi ancaman siber dari Tiongkok (Dolan, 2024).

Terciptanya hubungan trilateral mendorong diadakannya *training of foreign military and civilian defence personnel* yang mana Australia memperoleh pengembangan kapabilitas pertahanan siber melalui berbagai kegiatan pelatihan militer dan sipil di negara lain dibawah Pillar II AUKUS untuk memperkuat kapasitas Sumber Daya Manusia Australia melalui diplomasi pertahanan lewat transfer teknologi berupa pengetahuan, penelitian dan pengembangan teknologi bersama AS dan Inggris. Salah satu fokus pengembangan tersebut adalah teknologi siber berupa AI yang mencakup peningkatan ketahanan sistem otonom dan sistem yang didukung AI (Bae System, 2026). Implementasi pengembangan teknologi ini melalui Latihan Talisman Sabre tahun 2025 yang menggunakan algoritma AI ke sistem robotik dan otonom untuk melaksanakan misi intelijen, pengawasan dan pengintaian serta simulasi serangan (Australian Government, n.d.). Selain itu pada September 2025 lima personel ADF terlibat dalam pengujian *Joint Cyber Hunt Kit* di Philadelphia, AS untuk menguji tiga *prototipe* perangkat pertahanan siber serta mereka melakukan peningkatan kemampuan siber melalui pertahanan siber kolaboratif seperti penelitian dan pengembangan bersama dengan mempromosikan proyek penelitian dan pengembangan yang berfokus pada pengembangan teknologi siber mutakhir untuk mempercepat inovasi agar memastikan setiap negara anggota tetap unggul dalam kemajuan keamanan siber; berbagi intelijen dan sumber daya dengan memfasilitasi berbagai intelijen dan sumber daya di antara negara anggota serta meningkatkan kemampuan kolektif mereka untuk mendeteksi, mencegah dan merespons ancaman siber secara efektif (AUKUS Forum, 2024; Australian Government, 2025). Australia menilai bahwa kerjasama ini berpotensi membantu mengatasi kesenjangan teknologi dan memperkuat sistem pertahanan siber dalam menghadapi berbagai ancaman termasuk ancaman yang berasal dari Tiongkok. Dengan demikian pelatihan, penelitian dan pengembangan kapasitas siber melalui Pillar II AUKUS menjadi bagian penting bagi Australia untuk meningkatkan kesiapan dan efektivitas pertahanan siber melalui diplomasi pertahanan sekaligus memperkuat hubungan aliansi ketiga negara tersebut (Bae System, 2026).

Terbentuknya kerjasama trilateral mendorong adanya pelatihan yang didukung oleh *provision of military equipment and other material aid* yang dibuktikan melalui Latihan Talisman Sabre tahun 2025 menunjukan pemanfaatan teknologi siber berbasis AI untuk mendukung sistem otonom seperti robot, drone dll dalam menjalankan misi tanpa campur tangan manusia dan mengurangi resiko serta meningkatkan fleksibilitas operasional dimana AI melalui algoritma AI digunakan untuk memproses data berskala besar, menghasilkan informasi yang dapat ditindaklanjuti dan mendukung pengambilan keputusan dalam lingkungan operasional yang dinamis (AUKUS Forum, 2024; Australian Government, n.d.). Kemitraan AUKUS juga melibatkan kerjasama dengan pemasok penting dalam rantai pasokan angkatan laut melalui penerapan perangkat keamanan siber canggih (*advanced tooling*) bertujuan untuk meningkatkan keamanan rantai pasok dan memberikan pengetahuan tentang ancaman terhadap AUKUS dengan demikian kerjasama ini berpotensi memperkuat kemampuan pertahanan siber mereka khususnya dalam melindungi sistem komunikasi, operasi militer dan infrastruktur penting dari ancaman siber Tiongkok. Penguatan kerjasama AUKUS didukung oleh lingkungan perdagangan pertahanan bebas lisensi yang telah berlaku sejak 1 September 2024 dimana memungkinkan sektor industri, pendidikan tinggi dan penelitian di ketiga negara dapat melakukan ekspor dan memasok sebagian besar barang, teknologi dan layanan militer maupun *dual-use* antarnegara anggota tanpa memerlukan izin maupun lisensi. Sejalan dengan hal tersebut Strategi Pertahanan Nasional Australia menerapkan reformasi untuk mengintegrasikan perusahaan mereka ke dalam rantai pasokan global dan mendorong kolaborasi serta inovasi dalam pengembangan teknologi mutakhir (Australian Government, n.d.; Australian Government, 2023).

Dengan demikian partisipasi Australia melalui AUKUS menunjukan upaya mereka dalam memperkuat kemampuan pertahanan siber melalui kolaborasi teknologi dan pengamanan sistem pertahanan melalui pelatihan, penyediaan peralatan dan dukungan material

menjadi penghubung antara diplomasi pertahanan dan transfer teknologi siber di bawah Pillar II AUKUS karena adanya perpindahan pengetahuan, teknologi dan kemampuan teknis antarmitra untuk mendukung upaya menghadapi ancaman siber dari Tiongkok. Ketiga aktivitas diplomasi pertahanan menurut Cottey dan Foster memperlihatkan bagaimana diplomasi pertahanan Australia melalui AUKUS dapat mendukung transfer teknologi siber sebagai instrumen untuk memperkuat kapabilitas pertahanan siber kolektif dalam menghadapi berbagai ancaman termasuk ancaman yang berasal dari Tiongkok.

Transfer Teknologi Siber AUKUS Kepada Australia Sebagai Penguatan Pertahanan Siber Nasional Untuk Menghadapi Ancaman Siber Tiongkok.

Transfer teknologi merupakan pengembangan teknologi atau pengetahuan yang dilakukan di suatu lingkungan yang ditransfer untuk digunakan maupun dikembangkan di lingkungan yang lain (Choi, 2009). Proses transfer teknologi bertujuan untuk meningkatkan kapabilitas dan kinerja teknologi organisasi tertentu (Luna, n.d.). Dari definisi Choi dan Luna transfer teknologi didefinisikan sebagai perpindahan teknologi atau pengetahuan yang ditransfer ke sebuah lingkungan baru untuk dikembangkan atau digunakan dalam meningkatkan kapabilitas dan kinerja suatu mitra maupun organisasi. Transfer teknologi dibedakan menjadi dua jenis yaitu: transfer teknologi vertikal adalah transfer teknologi yang dihasilkan dari penelitian ke pengembangan dan produksi masing-masing sedangkan transfer teknologi horizontal adalah transfer teknologi yang proses membawa dan mengimplementasikan teknologi untuk dipakai di tempat yang berbeda. Model transfer teknologi menurut Schlie et al melalui tujuh elemen meliputi (1) pihak pemberi transfer, (2) pihak penerima transfer, (3) teknologi yang ditransfer, (4) mekanisme transfer, (5) lingkungan pemberi transfer, (6) lingkungan penerima transfer, dan (7) lingkungan besar yang mengelilingi pemberi maupun penerima transfer (Luna, n.d.).

Di era digital platform pertahanan dan infrastruktur kritis dll harus dilindungi oleh keamanan siber yang menjadi sebuah landasan dalam kedaulatan. Berdasarkan hal tersebut kemitraan AUKUS memberikan kemampuan transfer teknologi secara internasional karena berlangsung lintas tiga negara dilihat dari pembuatan kapal, sistem satelit hingga kecerdasan buatan (AI) setiap inisiatif AUKUS bergantung pada jaringan terpercaya, identitas terverifikasi dan ketahanan siber (AUKUS Forum, 2025). Jenis transfer teknologi AUKUS bersifat hibrida yang terdiri dari dua gabungan yaitu: transfer horizontal, melalui kemitraan ini penggunaan teknologi siber dari satu negara ke negara mitra untuk dikembangkan secara bersama sedangkan transfer vertikal ketika para negara anggota melakukan riset bersama dan melakukan pengembangan secara bertahap hingga tahap produksi untuk memperkuat pertahanan siber. Dilihat dari jenis transfer tersebut maka implikasi teknologi siber dijelaskan melalui model transfer teknologi menurut Schlie et al yang menjelaskan Amerika Serikat dan Inggris adalah pihak yang bekerjasama dengan Australia dalam pengembangan kemampuan teknologi canggih salah satunya *advanced cyber.* Disimpulkan bahwa Amerika Serikat dan Inggris ditempatkan sebagai pihak sumber kemampuan pengetahuan dan keahlian dalam kerjasama siber sedangkan Australia adalah pihak penerima yang berupaya memperoleh dan mengembangkan kemampuan tersebut sesuai dengan kebutuhan pertahanan nasionalnya namun transfer teknologi tidak hanya dipahami sebagai perpindahan perangkat teknologi secara fisik namun mencakup perpindahan pengetahuan, keterampilan dan pengalaman ketiga negara.

Mekanisme transfer teknologi siber melalui Latihan Talisman Sabre tahun 2025 ketika teknologi siber digunakan untuk mempercepat adopsi AI (algoritma AI) yang dilatih untuk merespons dan menganalisis informasi di *cyber domain* dan menyesuaikan pendekatan untuk mencapai suatu tugas dalam operasi pertahanan yang dapat meningkatkan keamanan siber dengan mendeteksi dan merespons ancaman lebih cepat dan memberikan perlindungan yang kuat dalam menganalisis data intelijen, mengidentifikasi pola dan data yang terlewatkan oleh

analis manusia sangat krusial untuk memahami pergerakan dan niat musuh (AUKUS Forum, 2024; Australian Government, n.d.). Disisi lain, keterlibatan Australia dalam pengujian dan evaluasi tiga *prototipe Joint Cyber Hunt Kit* bertujuan memperkuat pertahanan siber militer melalui pengetahuan yang didapatkan selama pelatihan berlangsung ADF dapat menerapkan kembali ke pangkalan komando mereka (*Departmen Of War Innovation Unit*, n.d.). Transfer teknologi kemitraan ini juga menerapkan perangkat keamanan siber canggih (*advanced tooling*) untuk meningkatkan keamanan rantai pasok dan pengetahuan akan ancaman dengan melakukan berbagi alat, teknik dan teknologi untuk melindungi jaringan keamanan nasional, sistem militer dan infrastruktur ekonomi dari ancaman siber (AUKUS Forum, 2024).

Amerika Serikat dan Inggris menjadi sumber lingkungan pemberi transfer melalui pengetahuan, pengalaman, keahlian serta kemampuan yang dikembangkan melalui kerjasama AUKUS alasannya karena kedua negara ini memiliki dominasi teknologi militer mutakhir, rekam jejak operasional selama puluhan tahun dan keunggulan riset pertahanan yang mungkin tidak dimiliki oleh Australia. Berdasarkan hal demikian maka Australia sebagai lingkungan penerima transfer untuk pertahanan dan keamanan siber akan menerima pengetahuan, keahlian dan pengalaman dll melalui kerjasama AUKUS untuk mendukung kapabilitas pertahanan dan keamanan siber Australia dalam meningkatkan kesiapan mereka dalam kemampuan uji coba, interoperabilitas dan kemampuan dalam menghadapi serta merespons ancaman siber. Dalam lingkungan yang lebih luas, adanya perkembangan kemampuan teknologi dan ancaman siber membuat para aktor untuk memperkuat kerjasama pertahanan dan keamanan siber di Indo-Pasifik sebagai pusat strategis geopolitik mengharuskan Australia untuk meningkatkan kemampuan pertahanan sibernya melaui kerjasama dengan AS dan Inggris. Dengan demikian model transfer teknologi dari Schlie et al menjelaskan transfer dan pengembangan kemampuan siber melalui kemitraan AUKUS berimplikasi terhadap penguatan pertahanan dan keamanan siber Australia yang memungkinkam kolaborasi dan kesinambungan dalam pengujian, pelatihan, dan operasi perburuan siber di seluruh pasukan ketiga negara mitra selain itu memberi kesempatan ADF untuk membawa ilmu yang diberikan dari AS kembali ke komando dan menyampaikan kemampuan yang sama demi meningkatkan interoperabilitas ADF (*Departmen Of War Innovation Unit,* n.d.).

Implementasi Transfer Teknologi Siber AUKUS Dalam Merespons Ancaman Siber Tiongkok

Di era modern keamanan nasional bukan hanya keamanan diranah konvensional yang melindungi kedaulatan negara secara fisik namun telah mencakup keamanan di ranah digital yang melindungi kedaulatan digital negara sehingga telah mengaburkan batas-batas tradisional membuat hal tersebut sangat penting. Menurut Joshi et al keamanan sekarang sudah berkaitan dengan keamanan siber di ruang siber untuk melindungi kedaulatan negara, infrastruktur kritis dan kemampuan pertahanan sebuah negara dari berbagai ancaman siber. Negara melindungi diri dengan menjaga pertahanannya berupa proteksi aset strategis pertahanan sekaligus mengamankan teknologi pertahanan meliputi teknologi digital untuk komunikasi, pengumpulan dan kontrol sistem senjata dll yang menghubungkan semuanya agar tidak menyebabkan kerentanan terhadap ancaman siber yang berdampak pada integritas operasional pertahanan suatu negara. Defenisi Boudy et al tentang keamanan siber dalam dimensi militer sebagai sebuah pendekatan modern dalam pertahanan melalui penggunaan teknologi baru di bidang militer meliputi sarana tempur, komando modern dan sistem komunikasi canggih yang berperan dalam peningkatan sistem tanpa awak dan otonom; platform senjata otomatis dan robotik berbasis AI dll sebagi penggunaan teknologi baru di bidang militer yang berimplikasi pada peningkatan kemampuan tempur, perlindungan dan ketahanan seperti ancaman siber yang menumbuhkan kesadaran situasional secara *real-time* melalui deteksi, pencegahan dan respons (Joshi, et al., 2025; Boudy, Janev, & Karpiuk, 2026).

Keamanan siber sangat penting bagi keamanan nasional Australia terhadap aktivitas ancaman siber dari Tiongkok di Indo-Pasifik, untuk merespons Tiongkok terhadap ancaman siber maka dibentuklah strategi pertahanan nasional sebagai respons Australia dalam membentuk kemitraan strategis bersama dengan AS dan Inggris di Indo-Pasifik untuk mengimbangi modernisasi militer dan strategi Tiongkok lewat transfer teknologi siber di bawah Pillar II AUKUS sebagai instrumen diplomasi pertahanan Australia untuk kepentingan strategisnya dalam penguatan kapabilitas pertahanan siber ADF. Kemampuan siber tingkat lanjut dalam kemitraan AUKUS menjelaskan bahwa keamanan siber di dunia yang saling terhubung saat ini karena itu transfer teknologi siber melalui integrasi pertahanan siber dibawah Pillar II AUKUS akan bekerjasama dan menggabungkan pendekatan untuk menarik dan mempertahankan ahli keamanan siber dan pengembangan sumber daya siber. Integrasi ini melibatkan latihan siber bersama melalui Latihan Talisman Sabre 2025, pengujian penetrasi pada tiga prototipe *Joint Cyber Hunt Kit*, berbagi intelijen ketiga negara dan informasi ancaman secara *real-time.*

Dengan demikian gabungan pendekatan tersebut melibatkan integrasi kemampuan kecerdasan buatan (AI), sistem otonom dan robotik dalam keamanan siber untuk peningkatan kemampuan tempur, perlindungan dan ketahanan seperti ancaman siber melalui deteksi, pencegahan dan respons. Namun disisi lain pendekatan dalam integrasi ini disatu sisi dapat menimbulkan kerentanan yang mana celah kerentanan dimanfaatkan Tiongkok dan APT untuk melakukan pencurian data, spionase, sistem dll oleh karena itu pertahanan siber yang terintegrasi menunjukan bahwa keamanan siber sangat penting untuk melindungi *cyber domain* dan infrastruktur penting melalui pengembangan tenaga kerja dan R&D (Dolan, 2024; AUKUS Forum, 2024).

KESIMPULAN DAN SARAN

Kesimpulan

Penelitian ini menunjukan bahwa diplomasi pertahanan Australia melalui kemitraan AUKUS, khususnya Pillar II berperan dalam memperkuat kapabilitas pertahanan siber Australia untuk merespons ancaman siber dari Tiongkok di Indo-Pasifik. Ancaman tersebut tercermin melalui aktivitas spionase, pencurian data, eksploitasi infrastruktur kritis, serta keterlibatan kelompok *Advanced Persistent Threat* (APT) yang terindikasi memiliki hubungan dengan kepentingan negara Tiongkok. Dalam menghadapi ancaman tersebut Australia memanfaatkan AUKUS sebagai instrumen diplomasi pertahanan melalui transfer teknologi siber yang melibatkan Amerika Serikat dan Inggris. Transfer teknologi tersebut berlangsung secara hibrida dan implementasinya diwujudkan melalui pelatihan bersama, pengembangan kecerdasan buatan (AI), pengujian tiga prototipe *Joint Cyber Hunt Kit*, pertukaran intelijen serta penggunaan perangkat keamanan siber canggih (*advanced tooling*). Temuan ini menunjukkan bahwa transfer teknologi tidak hanya mencakup perpindahan perangkat tetapi juga pengetahuan, keterampilan, pengalaman dan kemampuan teknis yang mendukung peningkatan interoperabilitas dan kapasitas Australia dalam mendeteksi, mencegah dan merespons ancaman siber. Dengan demikian penelitian ini memberikan kontribusi terhadap kajian hubungan internasional khususnya diplomasi pertahanan dan keamanan siber dengan menjelaskan bagaimana transfer teknologi dapat menjadi instrumen kerja sama pertahanan dalam menghadapi ancaman nonkonvensional di *cyber domain*. Adanya hubungan antara diplomasi pertahanan, transfer teknologi dan pertahanan keamanan siber dalam merespons ancaman siber Tiongkok, yang mana AUKUS memberikan peluang bagi Australia untuk mendapatkan teknologi canggih yang tidak dimiliki Australia sebelumnya, meningkatkan kesiapan personel pertahanan, memperkuat perlindungan infrastruktur kritis serta meningkatkan kemampuan operasional dalam menghadapi ancaman siber.

Keterbatasan

Penelitian ini memiliki beberapa keterbatasan. Pertama, penelitian hanya mengkaji pada diplomasi pertahanan Australia melalui kemitraan AUKUS yang fokusnya pada kerja sama mekanisme transfer teknologi siber berupa pelatihan dan pengembangan bersama dll sehingga belum dapat menyatakan apakah teknologi siber yang ditransfer sudah berhasil menangkal ancaman siber Tiongkok secara real. Kedua, penelitian ini hanya berfokus pada implementasi kerjasama teknologi siber dibawah Pillar II AUKUS sebagai bagian dari penguatan kemampuan pertahanan siber untuk melindungi keamanan siber Australia.

Saran

Penelitian selanjutnya disarankan untuk lebih banyak mengkaji efektivitas transfer teknologi siber AUKUS melalui indikator yang lebih terukur seperti peningkatan kapasitas deteksi dan respons ancaman, kesiapan sumber daya manusia serta ketahanan infrastruktur kritis Australia.

Kontribusi Author

Penulis pertama bertanggung jawab atas perumusan teori dan konsep penelitian, serta pengumpulan, analisis dan penyusunan data naskah. Penulis kedua dan ketiga berkontribusi dalam pengembangan kerangka teori dan konsep, interpretasi hasil penelitian serta proses penyempurnaan naskah. Secara keseluruhan penulis telah membaca dan menyetujui versi akhir naskah yang diterbitkan.

AI Disclosure Statement

Penulis menyatakan bahwa naskah penelitian ini disiapkan, diteliti, ditulis, dan disunting secara mandiri tanpa menggunakan bantuan teknologi atau teknik kecerdasan buatan (AI).

REFERENSI

AUKUS Forum. (2024, Februari 3). *Advanced Cyber Capabilities: A Pillar Of The AUKUS Partnership*. Retrieved from https://aukusforum.com/aukus-news/f/advanced-cyber-capabilities-a-pillar-of-the-aukus-partnership

AUKUS Forum. (2024, Mei 28). *Advancing Cyber Capabilities: An AUKUS Strategic Advantage*. Retrieved from https://aukusforum.com/aukus-news/f/advancing-cyber-capabilities-an-aukus-strategic-advantage

AUKUS Forum. (2024, Februari 6). *Artificial Intelligence: Empowering The Future Of Defense*. Retrieved from https://aukusforum.com/aukus-news/f/artificial-intelligence-empowering-the-future-of-defense-the-au

AUKUS Forum. (2025, Agustus 6). *AUKUS, Cybersecurity & The Future Of Trusted Information Sharing*. Retrieved from AUKUS Forum: https://aukusforum.com/aukus-news/f/aukus-cybersecurity-the-future-of-trusted-information-sharing

Australian Government. (2023, Desember 2). *AUKUS Defense Ministers Meeting Joint Statement*. Retrieved from https://www.minister.defence.gov.au/statements/2023-12-02/aukus-defense-ministers-meeting-joint-statemen

Australian Government. (2024). *2024 National Defence Strategy And 2024 Integrated Investment Program*. Retrieved from https://www.defence.gov.au/about/strategic-planning/2024-national-defence-strategy-2024-integrated-investment-program

Australian Government. (2025, September 1). *Cyber Kits Keep Allies In The Hunt.* Retrieved from https://www.defence.gov.au/news-events/news/2025-09-01/cyber-kits-keep-allies-hunt

Australian Government. (2026). *2026 National Defence Strategy And 2026 Integrated Investment Program*. Retrieved from https://www.defence.gov.au/about/strategic-planning/2026-national-defence-strategy-2026-integrated-investment-program

Australian Government. (n.d.). *AUKUS Advanced Capabilities*. Retrieved from https://www.defence.gov.au/defence-activities/programs-initiatives/aukus-advanced-capabilities

Australian Government. (n.d.). *Capability Achievements*. Retrieved from https://www.defence.gov.au/defence-activities/programs-initiatives/aukus-advanced-capabilities/capability-achievements

Australian Government. (n.d.). *Industry Engagement*. Retrieved from https://www.defence.gov.au/defence-activities/programs-initiatives/aukus-advanced-capabilities/industry-engagement

Australian, Governance. (2025, Oktober 14). *Annual Cyber Threat Report 2024-2025*. Retrieved from Australian Signals Directorate (ASD): https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2024-2025#:~:text=Annual%20Cyber%20Threat%20Report%202024%2D2025.

Australian, Governance. (2025, Agustus 28). *Countering Chinese State-Sponsored Actors Compromise Of Networks Worldwide To Feed Global Espionage System*. Retrieved from Australian Signals Directorate (ASD): https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/countering-chinese-state-sponsored-actors-compromise-of-networks-worldwide-to-feed-global-espionage-system#:~:text=Cybersecurity%20Industry%20Tracking%20*%20Salt%20Typhoon%2C%20*,*%2

Bae System. (2026, Maret 23). *AUKUS 'Pillar 2': Enhancing Collective Cyber Capabilities*. Retrieved from Bae System: https://careers.baesystems.com/insight/aukus-pillar-2-enhancing-collective-cyber-capabilities

Baram, G. (2025, September 15). *Chinese Cyber Skirmishes In The Indo-Pacific Show Emerging Patterns Of Conflict*. Retrieved from Australian Strategic Policy Institute (ASPI): https://www.aspistrategist.org.au/chinese-cyber-skirmishes-in-the-indo-pacific-show-emerging-patterns-of-conflict/#:~:text=The%20Indo%2DPacific%20has%20become,:%20Chor%20Muang/Getty%20Images.&text=Opinions%20in%20The%20Strategist%20are%20the%20authors%27%

Boudy, P. A., Janev, M. H., & Karpiuk, M. (2026, Juni 24). *The Military Dimension Of Cybersecurity*. Retrieved from Studia Luridica Lublinensia: https://journals.umcs.pl/sil/article/view/19499/pdf

Brathwaite, O. (2025). *A Cyber-Domain Escalation Framework*. Retrieved from https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1000&context=irps

Choi, H. J. (2009, Januari). *Technology Transfer Issues And A New Technology Transfer Model*. Retrieved from The Journal Of Technology Studies: https://www.researchgate.net/publication/281579422_pTechnology_Transfer_Issues_and_a_New_Technology_Transfer_Modelp

Cottey, A., & Forster, A. (2004). *Reshaping Defence Diplomacy: New Roles For Military Cooperation And Assistance*. Retrieved from Routledge: https://doi.org/10.4324/9781315000817

Cyber Capabilities Data. (2025). Retrieved from Lowy Institute Asia Power Index .

Darumaya, B. A., Maarif, S., Toruan, T., & Swastanto, Y. (2023, Desember 26). *Thouhts On The Potential Threat Of Cyber War In Indonesia: A Defense Strategy Study*. Retrieved from Jurnal Keamanan Nasional: https://ejurnal.ubharajaya.ac.id/index.php/kamnas/article/view/1418/1096

Departmen Of War Innovation Unit. (n.d.). *Solutions Selected To Increase Resilience Of Critical Networks*. Retrieved from Departmen Of War Innovation Unit (DIU): https://www.diu.mil/latest/solutions-selected-to-increase-resilience-of-critical-networks

Dohr, P. (2025, Desember 1). *China's Weaponizations Of Global Cyber Supply Chains*. Retrieved from Center For Strategic & International Studies (CSIS): https://www.csis.org/blogs/strategic-technologies-blog/chinas-weaponization-global-cyber-supply-chains

Dolan, C. J. (2024, Mei 8). *Perspective Chapter: AUKUS Pillar 2 Technologyy, Interoperability, And Advanced Capabilities In The Evolving Trilateral Security Partnership*. Retrieved from National Security In The Digital And Information Age: https://www.intechopen.com/chapters/1175322

Effendy, R. K. (2025, Oktober 3). *Perkembangan Siber Dan Dominasi Teknologi Militer China Dalam Geopolitik Di Kawasan*. Retrieved from Diplomacy And Global Security Journal: https://ejournal.fisip.unjani.ac.id/index.php/DGSJ/article/view/4622/1212

Galinec, D., Moznik, D., & Guberina, B. (2018, Januari 25). *Cybersecurity And Cyber Defence: National Level Strategic Approach*. Retrieved from Journal For Control, Measurement, Electronics, Computing And Communications: https://www.tandfonline.com/doi/full/10.1080/00051144.2017.1407022#d1e173

Given, L. M. (2008). *The Sage Ecnyclopedia Of Qualitative Research Methods*. Retrieved from SAGE Publications, inc.: https://methods.sagepub.com/ency/edvol/sage-encyc-qualitative-research-methods/toc#_

ITU. (2024, September 12). *Countries Strengthening Cybersecurity Efforts, But Increased Action Still Required*. Retrieved from International Telecommunication Union: https://www.itu.int/en/mediacentre/Pages/PR-2024-09-10-Global-Cybersecurity-Index.aspx

Joshi, N. V., P, S., Patra, S., Prasad, R. S., Sayyed, J. K., Das, A., & Manjunath, T. (2025, Oktober). *Cybersecurity And National Security: The Growing Significance Of Digital Threats And Their Ramifications For National Security*. Retrieved from Research Gate: https://www.researchgate.net/publication/397630697_Cybersecurity_and_National_Security_The_Growing_Significance_of_Digital_Threats_and_Their_Ramifications_for_National_Security

Lubis, L. A., Perwita, A. B., & Hadisancoko, R. E. (2024, Agustus). *The Role of AUKUS in Australia's Military Capacity Building Strategy*. Retrieved from International Journal Of Society And Law: https://journal.ysmk.or.id/index.php/IJSL/article/view/128#:~:text=AUKUS%2C%20was%20established%20to%20increase%20Australia%27s%20defense,AUKUS%20addresses%20Australia%27s%20pre%2Dexisting%20military%20challenges%20by

Luna, N. D. (n.d.). *Understanding Technology Transfer: Its Facts And Models*. Retrieved from Academia.edu: https://www.academia.edu/14149178/Understanding_Technology_Transfer_Its_Facts_and_Models.

Mo, L. (2025, Mei 12). *新时代的中国国家安全 (China's National Security In The New Era)*. Retrieved from The State Council Information Office Of The People's Republic Of China: http://www.scio.gov.cn/zfbps/zfbps_2279/202505/t20250512_894771.html

Siroli, G. P. (2018, Mei 29). *Considerations On The Cyber Domain As The New Worldwide Battlefield*. Retrieved from Italian Journal Of International Affairs: https://www.tandfonline.com/doi/abs/10.1080/03932729.2018.1453583

Siswoyo, A. (2025, Oktober 3). *Pengembangan Kapasitas Militer Australia Dalam Menghadapi Tantangan Keamanan China Tahun 2022-2024*. Retrieved from Diplomacy And Global Security Journal: https://ejournal.fisip.unjani.ac.id/index.php/DGSJ/article/view/4618/1217

The People's Republic Of China. (2019, July 24). *China's National Defense In The New Era*. Retrieved from

https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html

Thekkekara, L. V. (2025, Desember 19). *Australian Defence Technologies Amidst Shifting Global Economic Dynamics*. Retrieved from Contemporary Issues In Air & Space Power: https://ciasp.scholasticahq.com/article/147830-australian-defence-technologies-amidst-shifting-global-economic-dynamics

Wibisono, I., Mahroza, J., & Poespitohadi, W. (2019, Januari). *Diplomasi Pertahanan Indonesia Dalam Meningkatkan Industri Pertahanan (Studi Kasus Joint Development Medium Tank Indonesia Dengan Turki)*. Retrieved from Research Gate: https://www.researchgate.net/publication/397940778_FULL_THESIS_DIPLOMASI_PERTAHANAN_INDONESIA_DALAM_MENINGKATKAN_INDUSTRI_PERTAHANAN_STUDI_KASUS_JOINT_DEVELOPMENT_MEDIUM_TANK_INDONESIA DENGANTURKIpdf

Zainuddin, I., & Wardhana, A. (2024, Juli). *Teknik Pengumpulan Data Penelitian*. Retrieved from Eureka Media Aksara: https://www.researchgate.net/publication/382060598_Teknik_Pengumpulan_Data_Penelitian