DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 2, No. 2 Tahun 2026 Hal. 176-193
e-ISSN: 3110-6048 DOI: 10.36859/dgsj.v2i2.5620

Article History:
Submitted:Feb 20, 2026
Accepted: Mar 21, 2026
Published: Apr 28, 2026

DAMPAK STRATEGI CYBER WARFARE CHINA DALAM UPAYA MENINGKATKAN PENGARUHNYA TERHADAP STABILITAS KEAMANAN DI INDO PASIFIK

Mohammad Misbahul Munir[1]

1. Program Studi Magister Hubungan Internasional Universitas Jenderal Achmad Yani, Cimahi, Indonesia

ABSTRACT

This study aims to analyze China's cyber warfare strategy in its efforts to expand geopolitical influence in the Indo-Pacific region and to examine the implications of China's military technological dominance for regional security stability. The rapid development of digital technology and cyber capabilities has transformed cyberspace into a strategic instrument in global power competition. This research employs a qualitative method through literature review, document analysis, and the examination of relevant academic and policy sources. The analysis is conducted using the perspectives of Realism, Security Dilemma Theory, Power Transition Theory, and Regional Security Complex Theory.

The findings indicate that China utilizes cyber warfare strategies through cyber espionage, hacking operations, digital disinformation campaigns, and the advancement of information and communication technologies to strengthen its political, economic, and security influence in the Indo-Pacific. Furthermore, China's military technological dominance, supported by developments in artificial intelligence, 5G networks, and military modernization, has enhanced its strategic position as a major regional power. However, these developments have also prompted security responses from countries such as the United States, Japan, India, and Australia, which have intensified their defense cooperation and cybersecurity partnerships. This situation has generated a security dilemma that increases regional tensions and contributes to an emerging arms race. The study concludes that China's cyber warfare strategy and military technological dominance have become key instruments for expanding its geopolitical influence while simultaneously creating new challenges for the security and stability of the Indo-Pacific region.

Keywords: Cyber Warfare, China, Indo-Pacific, Security Stability, Military Technological Dominance, Geopolitics.

ABSTRAK

Penelitian ini bertujuan untuk menganalisis strategi cyber warfare yang diterapkan China dalam upaya meningkatkan pengaruh geopolitiknya di kawasan Indo-Pasifik serta mengkaji implikasi dominasi teknologi militer China terhadap stabilitas keamanan kawasan. Perkembangan teknologi digital dan meningkatnya kapabilitas siber telah menjadikan ruang siber sebagai instrumen strategis dalam persaingan kekuatan global. Penelitian ini menggunakan metode kualitatif dengan pendekatan studi pustaka, analisis dokumen, dan kajian berbagai literatur yang relevan. Analisis dilakukan dengan menggunakan pendekatan Realisme, Teori Security Dilemma, Teori Kebangkitan Kekuatan (Power Transition Theory), serta Teori Kompleks Keamanan Regional (Regional Security Complex Theory).

Hasil penelitian menunjukkan bahwa China memanfaatkan strategi cyber warfare melalui operasi spionase siber, peretasan, disinformasi digital, serta pengembangan teknologi informasi dan komunikasi untuk memperluas pengaruh politik, ekonomi, dan keamanan di kawasan Indo-Pasifik. Selain itu, dominasi teknologi militer China yang didukung oleh pengembangan kecerdasan buatan, jaringan 5G, dan modernisasi sistem persenjataan telah meningkatkan posisi strategis China sebagai kekuatan regional yang berpengaruh. Namun, kondisi tersebut juga memicu respons keamanan dari negara-negara lain seperti Amerika Serikat, Jepang,

DIPLOMACY AND GLOBAL SECURITY JOURNAL **Jurnal Mahasiswa Magister Hubungan Internasional** **Vol. 2, No. 2 Tahun 2026 Hal. 176-193** **e-ISSN: 3110-6048 DOI: 10.36859/dgsj.v2i2.5620**	Article History: *Submitted:Feb 20, 2026* *Accepted: Mar 21, 2026* *Published: Apr 28, 2026*

India, dan Australia yang memperkuat kerja sama pertahanan dan keamanan siber mereka. Situasi ini menciptakan dinamika security dilemma yang berpotensi meningkatkan ketegangan dan perlombaan senjata di kawasan. Penelitian ini menyimpulkan bahwa strategi cyber warfare dan dominasi teknologi militer China telah menjadi instrumen penting dalam memperluas pengaruh geopolitiknya, sekaligus menimbulkan tantangan baru bagi stabilitas keamanan kawasan Indo-Pasifik.

Kata Kunci: Cyber Warfare, China, Indo-Pasifik, Stabilitas Keamanan, Dominasi Teknologi Militer, Geopolitik.

PENDAHULUAN

Internet dapat dianggap sebagai salah satu inovasi paling revolusioner dalam sejarah modern. Kehadirannya telah memungkinkan kita untuk melakukan hal-hal yang sebelumnya dianggap mustahil dan, yang lebih penting, telah menjadikan dunia kita lebih terhubung dari sebelumnya. Sejak munculnya internet, hampir setiap aspek kehidupan manusia mengalami perubahan signifikan, termasuk dalam hubungan diplomatik antarnegara. Selain itu, internet juga berperan dalam mengubah dinamika peperangan, menciptakan dimensi baru dalam pertahanan dan keamanan global.[1] Untuk menghadapi perubahan besar ini, negara-negara di seluruh dunia telah berlomba-lomba memperkuat kapabilitas siber mereka guna tetap kompetitif di kancah internasional. Beberapa negara adidaya telah menginvestasikan sumber daya yang besar dalam pengembangan sistem teknologi canggih, sementara negara-negara lain yang memiliki keterbatasan dana dan keahlian masih tertinggal dalam perlombaan ini. Salah satu negara yang menarik untuk dikaji adalah Tiongkok.[2] Meskipun awalnya tertinggal dibandingkan Rusia dan Amerika Serikat dalam pengembangan kemampuan siber, Tiongkok berhasil mengejar ketertinggalannya dengan pesat.

Berkaitan dengan hal tersebut, dalam beberapa tahun terakhir, dinamika geopolitik di kawasan Indo-Pasifik telah mengalami perubahan yang signifikan. Salah satu faktor utama yang mendorong perubahan ini adalah meningkatnya peran China dalam perang siber dan teknologi militer. China tidak hanya memperkuat posisinya sebagai kekuatan ekonomi global, tetapi juga secara agresif mengembangkan kapabilitas siber dan militernya untuk memperluas pengaruh di kawasan tersebut. Persaingan geopolitik antara China dan negara-negara lain, seperti Amerika Serikat, Australia, Jepang, dan negara-negara ASEAN, semakin mengarah pada rivalitas dalam ranah digital dan militer.

National Institute of Standards and Technology (NIST) dari Amerika Serikat mendefinisikan serangan siber sebagai segala bentuk aktivitas berbahaya yang bertujuan untuk mengakses, mengganggu, menolak, merusak, atau bahkan menghancurkan sistem informasi maupun data yang tersimpan di dalamnya.[3] Karena dunia siber masih terus

[1] Steven Feldstein, 2022. Disentangling The Digital Battlefield: How the Internet Has Changed War. Diakses melalui : https://warontherocks.com/2022/12/disentangling-the-digital-battlefield-how-theinternet-has-changed-war/

[2] Lyu Jinghua, 2022. What Are China's Cyber Capabilities and Intentions?. Diakses melalui : https://carnegieendowment.org/posts/2019/04/what-are-chinas-cyber-capabilities-andintentions?lang=en

[3] Peter Harrell, 2025. Managing the Risks of China's Access to U.S. Data and Control of Software and Connected Technology. Diakses melalui : https://carnegieendowment.org/research/2025/01/managing-the-risks-of-chinas-access-to-us-dataand-control-of-software-and-connected-technology?lang=en

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 2, No. 2 Tahun 2026 Hal. 176-193
e-ISSN: 3110-6048 DOI: 10.36859/dgsj.v2i2.5620

Article History:
Submitted:Feb 20, 2026
Accepted: Mar 21, 2026
Published: Apr 28, 2026

berkembang, pemahaman mengenai serangan siber pun beragam, dengan berbagai definisi dan perspektif yang terus diperbarui seiring waktu. Meskipun begitu, ada beberapa bentuk serangan siber yang paling umum dan sering terjadi. Pertama, pencurian data, di mana peretas mengakses dan mencuri informasi sensitif dari sistem tertentu. Data yang dicuri ini dapat diperjualbelikan, dimanfaatkan untuk kepentingan intelijen, atau bahkan digunakan untuk pemerasan. Kedua, destabilisasi, yaitu serangan langsung terhadap pemerintah atau infrastruktur suatu negara dengan tujuan menciptakan ketidakstabilan sosial dan politik. Ketiga, gangguan ekonomi, di mana bank, perusahaan keuangan, atau lembaga bisnis menjadi target untuk pencurian dana maupun manipulasi sistem ekonomi.

Keempat, serangan propaganda, yaitu upaya memanipulasi opini publik di negara lain dengan menyebarkan disinformasi atau narasi tertentu yang dapat memengaruhi kebijakan dan perilaku masyarakat. Terakhir, sabotase, yang sering kali berkaitan dengan peperangan konvensional maupun non-konvensional. Dalam skenario ini, serangan siber ditujukan untuk melumpuhkan sistem komputer pemerintah, infrastruktur penting, atau perangkat militer guna melemahkan kekuatan lawan.

Meningkatnya aktivitas siber China menimbulkan tantangan baru dalam keamanan regional. Pada tahun 2023, berbagai laporan mengungkapkan bahwa China diduga berada di balik serangkaian serangan siber yang menargetkan infrastruktur kritis di berbagai negara, termasuk Vietnam, Indonesia, dan Taiwan.[4] Selain itu, Taiwan tetap menjadi fokus utama bagi para peretas China karena kepentingan strategisnya dalam kebijakan "Satu China". Serangan ini tidak hanya menimbulkan kerugian ekonomi, tetapi juga mengancam stabilitas politik dan keamanan regional. Jenis peperangan modern berbasis teknologi ini bukanlah hal baru bagi Tentara Pembebasan Rakyat Tiongkok (PLA). Selama bertahun-tahun, PLA telah aktif meningkatkan kemampuan persenjataan berbasis informasi serta teknologi militernya guna menghadapi tantangan di era digital.

Dalam Bab III dari *Buku Putih Pertahanan Nasional Tiongkok tahun 2004*, yang berjudul *Revolusi dalam Urusan Militer dengan Karakteristik Tiongkok*, otoritas Tiongkok secara terbuka menyatakan ambisi mereka untuk mengembangkan persenjataan berteknologi tinggi. Tidak hanya sekadar meningkatkan kapasitas militer, mereka juga mengumumkan rencana strategis untuk merekrut serta melibatkan individu-individu paling berbakat di negara itu dalam pengembangan sistem pertahanan berbasis teknologi canggih.[5] Langkah ini mencerminkan komitmen Tiongkok dalam membangun kekuatan militer yang tidak hanya bergantung pada kekuatan konvensional, tetapi juga memanfaatkan teknologi mutakhir dalam peperangan siber dan sistem persenjataan berbasis informasi. Dengan strategi ini, Tiongkok bertujuan untuk memastikan bahwa mereka tetap kompetitif dalam lanskap militer global yang semakin bergeser ke arah digitalisasi dan otomatisasi.

Meningkatnya aktivitas siber dan ekspansi militer China menimbulkan beberapa permasalahan utama. Pertama, munculnya ancaman terhadap kedaulatan digital negara-

[4] UNAV. (2023). *Chinese Cyber Warfare in the Indo-Pacific*. University of Navarra. Diakses melalui : https://www.unav.edu/web/global-affairs

[5] China People's Liberation Army, 2004. China White Paper. Diakses melalui : http://www.china.org.cn/e-white/20041227/III.htm#5

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 2, No. 2 Tahun 2026 Hal. 176-193
e-ISSN: 3110-6048 DOI: 10.36859/dgsj.v2i2.5620

Article History:
Submitted:Feb 20, 2026
Accepted: Mar 21, 2026
Published: Apr 28, 2026

negara di Indo-Pasifik. Serangan siber yang dilakukan China diduga bertujuan untuk memperoleh informasi strategis, mengganggu stabilitas politik, serta memperlemah posisi ekonomi negara-negara target. Kedua, adanya potensi eskalasi konflik di Laut China Selatan akibat dominasi militer China. Persaingan antara China dan Amerika Serikat semakin memanas, dan ini dapat berdampak pada negara-negara di kawasan yang memiliki hubungan erat dengan kedua kekuatan besar tersebut. Selain itu, tantangan dalam regulasi internasional mengenai perang siber masih menjadi masalah yang belum terselesaikan. Saat ini, belum ada norma yang secara jelas mengatur bagaimana negara harus bertindak dalam menghadapi ancaman siber yang bersifat lintas batas. Hal ini membuka celah bagi negara-negara untuk menggunakan perang siber sebagai alat politik dan ekonomi.

Selain itu, Cina telah mengembangkan beberapa cara untuk menghindari menjadi target serangan siber. Terlepas dari kemampuan teknis dan teknologi yang dapat dikumpulkannya, para pemimpin Tiongkok juga khawatir tentang perselisihan hukum dan urusan yang dapat mereka hadapi untuk melemahkan kemungkinan diretas atau dimata-matai. Salah satu inisiatif ini adalah UndangUndang Keamanan Siber Tiongkok yang diberlakukan pada tahun 2017, memberikan kerangka kerja peraturan dan kewajiban tertentu untuk penggunaan data, yang juga diterapkan secara ketat untuk perusahaan asing yang bekerja di Tiongkok. Selain itu, pada bulan Maret 2023, pemerintah Tiongkok menerbitkan buku putih, 'Tata Kelola Dunia Maya Berbasis Hukum Tiongkok di Era Baru', di mana Tiongkok mengusulkan kerangka kerja peraturan internasional tentang topik keamanan siber.[6]

Dalam konteks realitas yang ada, China telah berhasil membangun kapabilitas siber dan militer yang mumpuni serta memperluas pengaruhnya di kawasan Indo-Pasifik.[7] China secara aktif mengembangkan teknologi kecerdasan buatan (AI), jaringan 5G, dan persenjataan canggih untuk memperkuat dominasinya. Namun, idealnya, diperlukan mekanisme internasional yang dapat memastikan bahwa perkembangan ini tidak mengancam stabilitas regional dan menghormati kedaulatan negara-negara lain. Negara-negara di kawasan IndoPasifik harus meningkatkan kerja sama dalam bidang keamanan siber dan militer untuk menghadapi ancaman yang semakin kompleks.

Untuk menganalisis fenomena ini, teori Geopolitik Klasik dapat diterapkan. Teori ini menekankan pentingnya faktor geografis dan kekuatan militer dalam menentukan dominasi global. Menurut teori ini, negara dengan penguasaan wilayah strategis akan memiliki keuntungan dalam persaingan global. Dalam hal ini, Laut China Selatan menjadi area kunci dalam strategi geopolitik China. Selain itu, teori Kompleks Keamanan Regional (*Regional Security Complex Theory*) juga relevan untuk memahami bagaimana keamanan di Indo-Pasifik saling berhubungan.[8] Teori ini menjelaskan bahwa keamanan suatu negara tidak dapat dipisahkan dari dinamika keamanan di kawasan sekitarnya. Dengan meningkatnya

[6] Universidad de Navarra, 2023. Chinese Cyber Warfare in the Indo-Pacific: An analysis of means, targets, and solutions. Diakses melalui : https://www.unav.edu/web/global-affairs/chinese-cyberwarfare-in-the-indo-pacific
[7] Publikasi Ilmiah UNWAHAS. (2023). *Analisis Strategi Keamanan Siber China di Kawasan IndoPasifik*. Diakses melalui: https://publikasiilmiah.unwahas.ac.id
[8] Buzan, B., & Waever, O. (2003). *Regions and Powers: The Structure of International Security*. Cambridge: Cambridge University Press.

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 2, No. 2 Tahun 2026 Hal. 176-193
e-ISSN: 3110-6048 DOI: 10.36859/dgsj.v2i2.5620

Article History:
Submitted:Feb 20, 2026
Accepted: Mar 21, 2026
Published: Apr 28, 2026

aktivitas siber dan militer China, negara-negara di Indo-Pasifik harus merespons dengan memperkuat kerja sama keamanan dan membangun strategi pertahanan yang lebih kokoh.

KERANGKA ANALITIK

Pendekatan Realisme

Pendekatan realisme merupakan salah satu teori utama dalam studi hubungan internasional. Pendekatan ini menekankan pada aspek kekuasaan dan kepentingan nasional sebagai faktor utama yang menggerakkan interaksi antarnegara. Realisme berakar pada pemikiran bahwa dunia adalah arena konflik dan persaingan, di mana setiap negara bertindak berdasarkan kepentingan sendiri demi bertahan hidup dalam sistem internasional yang anarkis. Pandangan ini muncul sebagai respons terhadap idealisme yang dianggap terlalu optimistis dalam melihat kemungkinan kerja sama antarnegara.

Sejarah realisme dapat ditelusuri sejak zaman kuno, dengan Thucydides sebagai salah satu pemikir awal yang menuliskan bagaimana dinamika kekuasaan mempengaruhi hubungan antarnegara dalam Perang Peloponnesian. Dalam karyanya, ia menyoroti bagaimana negara-negara bertindak demi kepentingan mereka sendiri tanpa memperhitungkan aspek moralitas. Pemikiran ini kemudian diteruskan oleh Niccolò Machiavelli, yang dalam karyanya *The Prince* menggambarkan pentingnya kelicikan dan kekuasaan dalam mempertahankan negara. Pemikir lainnya, Thomas Hobbes, dalam *Leviathan*, mengembangkan gagasan bahwa dalam kondisi tanpa pemerintahan yang kuat, manusia akan berada dalam keadaan perang semua melawan semua, sebuah prinsip yang kemudian diterapkan dalam analisis hubungan internasional.

Pada abad ke-20, realisme berkembang menjadi teori yang lebih sistematis dengan karya-karya seperti *Politics Among Nations* oleh Hans Morgenthau. Morgenthau menekankan bahwa kepentingan nasional harus selalu didefinisikan dalam istilah kekuasaan, dan bahwa politik internasional adalah perjuangan terus-menerus untuk mempertahankan atau meningkatkan kekuasaan. Morgenthau menolak pendekatan normatif yang mencoba membangun tatanan dunia berdasarkan prinsip moralitas universal dan menegaskan bahwa hubungan internasional lebih dipengaruhi oleh faktor rasional dan kalkulatif.

Realisme kemudian mengalami perkembangan lebih lanjut melalui pemikiran Kenneth Waltz yang memperkenalkan neorealisme atau realisme struktural. Dalam *Theory of International Politics*, Waltz menegaskan bahwa bukan hanya sifat manusia atau keinginan negara individu yang menentukan perilaku dalam sistem internasional, tetapi struktur sistem internasional itu sendiri. Dengan kata lain, anarki dalam sistem internasional memaksa negara-negara untuk bertindak dengan cara tertentu demi bertahan hidup, sehingga persaingan kekuatan menjadi tidak terhindarkan. Pendekatan ini lebih menekankan pada bagaimana distribusi kekuasaan dalam sistem internasional menentukan perilaku negara, daripada sekadar melihat keputusan yang dibuat oleh individu pemimpin atau elit politik.

Perkembangan lebih lanjut dari realisme juga terjadi dengan munculnya realisme ofensif yang dikembangkan oleh John Mearsheimer. Dalam *The Tragedy of Great Power Politics*, Mearsheimer berargumen bahwa negara-negara tidak hanya berusaha mempertahankan kekuasaan mereka, tetapi juga secara aktif berusaha meningkatkan kekuatan mereka untuk mencapai dominasi. Dalam pandangan ini, keamanan hanya dapat

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 2, No. 2 Tahun 2026 Hal. 176-193
e-ISSN: 3110-6048 DOI: 10.36859/dgsj.v2i2.5620

Article History:
Submitted:Feb 20, 2026
Accepted: Mar 21, 2026
Published: Apr 28, 2026

dijamin dengan menjadi kekuatan terbesar dalam sistem internasional, sehingga negara-negara akan selalu mencari cara untuk memperbesar pengaruh dan kekuatan mereka.

Pendekatan realisme tetap menjadi perspektif dominan dalam studi hubungan internasional karena kemampuannya dalam menjelaskan berbagai dinamika geopolitik, konflik, dan persaingan kekuatan yang terjadi sepanjang sejarah. Dari perang dunia hingga Perang Dingin dan persaingan kekuatan besar saat ini, realisme terus digunakan sebagai kerangka kerja untuk memahami bagaimana negara-negara bertindak dalam sistem internasional yang anarkis. Sementara pendekatan lain seperti liberalisme dan konstruktivisme mencoba memberikan alternatif dalam memahami hubungan internasional, realisme tetap menjadi teori yang paling relevan dalam menjelaskan aspek kekuasaan dan kepentingan nasional yang mendominasi politik dunia.

Dalam konteks modern, pendekatan realisme juga dapat diterapkan dalam analisis perkembangan teknologi siber dan dominasi teknologi militer China dalam geopolitik kawasan. Sebagai negara dengan ambisi global, China menggunakan strategi realistis dalam memperkuat kemampuan siber dan militernya sebagai alat untuk menegaskan kekuatan serta mempertahankan kepentingan nasionalnya. Dominasi teknologi ini tidak hanya menciptakan keseimbangan kekuatan baru tetapi juga meningkatkan ketegangan dengan negara-negara pesaing seperti Amerika Serikat. Dalam perspektif realisme, penguatan kapabilitas militer berbasis teknologi tinggi merupakan langkah strategis yang diambil oleh negara-negara untuk mengamankan posisi mereka dalam sistem internasional yang kompetitif. Pendekatan realisme akan memudahkan peneliti dalam mengkaji lebih mendalam mengenai judul yang diangkat.

Teori Security Dilemma

Security dilemma atau dilema keamanan merupakan konsep kunci dalam studi hubungan internasional, khususnya dalam pendekatan realisme. Konsep ini menjelaskan bagaimana upaya suatu negara untuk meningkatkan keamanannya justru dapat menimbulkan ketidakamanan bagi negara lain, sehingga memicu spiral ketegangan dan persaingan militer. Security dilemma muncul sebagai akibat dari struktur anarkis sistem internasional, di mana tidak ada otoritas pusat yang dapat menjamin keamanan absolut bagi semua negara. Oleh karena itu, setiap negara cenderung mengadopsi strategi bertahan dengan memperkuat kapabilitas militernya, yang pada akhirnya dapat dianggap sebagai ancaman oleh pihak lain.

Security dilemma pertama kali dikemukakan oleh John H. Herz pada tahun 1950 dan kemudian diperjelas oleh pemikir seperti Herbert Butterfield dan Robert Jervis. Herz menyatakan bahwa dalam lingkungan internasional yang anarkis, negara-negara tidak dapat sepenuhnya mempercayai niat pihak lain, sehingga mereka merasa perlu untuk terus meningkatkan kemampuan pertahanan mereka. Hal ini sering kali mengarah pada perlombaan senjata, bahkan ketika tidak ada niat agresi yang jelas dari pihak mana pun.[9] Konsep ini berakar dalam pemikiran realisme, yang menekankan bahwa negara bertindak dalam kondisi ketidakpastian dan selalu berusaha mengamankan kepentingannya.

[9] Herz, J. H. (1950). *Political Realism and Political Idealism: A Study in Theories and Realities*. Chicago: University of Chicago Press.

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 2, No. 2 Tahun 2026 Hal. 176-193
e-ISSN: 3110-6048 DOI: 10.36859/dgsj.v2i2.5620

Article History:
Submitted:Feb 20, 2026
Accepted: Mar 21, 2026
Published: Apr 28, 2026

Robert Jervis mengembangkan teori ini lebih lanjut dengan membedakan antara kemampuan ofensif dan defensif dalam strategi militer. Jika suatu negara mengembangkan sistem pertahanan yang sulit dibedakan antara tujuan ofensif dan defensifnya, maka kemungkinan terjadinya security dilemma semakin besar. Dalam konteks ini, negaranegara sering kali terjebak dalam situasi di mana mereka merasa harus terus meningkatkan kapasitas militernya untuk menghindari potensi serangan dari pihak lain, meskipun hal tersebut hanya memperburuk ketegangan.[10]

Security dilemma juga dapat diterapkan dalam berbagai konflik kontemporer, termasuk ketegangan antara Amerika Serikat dan China di kawasan Indo-Pasifik. Dengan meningkatnya pengaruh China dalam bidang teknologi militer dan siber, negara-negara lain seperti Amerika Serikat dan sekutunya di kawasan merasa terdorong untuk memperkuat aliansi dan meningkatkan kapabilitas pertahanan mereka. Ini terlihat dalam kebijakan penguatan militer di Laut China Selatan, peningkatan kerja sama keamanan di antara negara-negara Indo-Pasifik, serta berkembangnya strategi militer berbasis teknologi tinggi untuk menanggapi dominasi China.

Dalam perspektif security dilemma, pengembangan teknologi militer dan siber oleh China bukan hanya strategi untuk memperkuat pertahanan nasionalnya tetapi juga dapat dilihat sebagai langkah ofensif oleh negara lain. Misalnya, kemajuan dalam kecerdasan buatan, komputasi kuantum, serta penguatan kemampuan siber China telah menimbulkan kekhawatiran bagi negara-negara pesaingnya. Hal ini mendorong respons yang serupa dari negara-negara lain, sehingga mempercepat dinamika perlombaan teknologi militer yang semakin kompleks dan sulit dikendalikan.

Secara keseluruhan, security dilemma tetap menjadi teori yang relevan dalam memahami dinamika geopolitik modern. Dengan semakin berkembangnya teknologi militer dan perang siber, security dilemma semakin diperumit oleh faktor-faktor non-tradisional dalam keamanan internasional. Ketika negara-negara terus berusaha memperkuat pertahanannya, mereka juga menghadapi tantangan baru dalam mencegah eskalasi konflik yang tidak diinginkan.

Teori Kebangkitan Kekuatan (Power Transition Theory)

Teori Kebangkitan Kekuatan (Power Transition Theory) adalah salah satu teori penting dalam hubungan internasional yang berusaha menjelaskan dinamika perubahan kekuatan global dan potensi konflik yang muncul ketika kekuatan baru bangkit untuk menantang kekuatan dominan yang ada. Teori ini pertama kali dikembangkan oleh A.F.K.

Organski pada akhir 1950-an dalam bukunya World Politics (1958), dan kemudian diperluas oleh para sarjana seperti Jacek Kugler dan Ronald L. Tammen. Teori ini menawarkan perspektif yang berbeda dari realisme klasik, terutama dalam hal penekanannya pada hierarki kekuasaan dan peran kepuasan status quo dalam menjaga stabilitas internasional.[11]

[10] Jervis, R. (1978). *Cooperation Under the Security Dilemma*. World Politics, 30(2), 167-214.
[11] Organski, A.F.K. (1958). *World Politics*. New York: Knopf.

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 2, No. 2 Tahun 2026 Hal. 176-193
e-ISSN: 3110-6048 DOI: 10.36859/dgsj.v2i2.5620

Article History:
Submitted:Feb 20, 2026
Accepted: Mar 21, 2026
Published: Apr 28, 2026

Teori Kebangkitan Kekuatan berargumen bahwa sistem internasional tidak sepenuhnya anarkis, melainkan terstruktur dalam hierarki kekuasaan.[12] Negara-negara ditempatkan dalam hierarki ini berdasarkan kekuatan relatif mereka, yang diukur melalui faktor-faktor seperti kekuatan ekonomi, militer, dan kapabilitas teknologi. Di puncak hierarki ini terdapat negara hegemon atau kekuatan dominan yang memegang kendali atas sistem internasional. Negara hegemon ini biasanya menetapkan aturan dan norma yang menguntungkan dirinya, dan negaranegara lain harus mematuhi aturan ini jika mereka ingin mempertahankan stabilitas.[13] Namun, hierarki ini tidak statis. Seiring waktu, negara-negara yang lebih kecil atau menengah dapat mengalami pertumbuhan ekonomi dan militer yang signifikan, sehingga mereka naik dalam hierarki kekuasaan. Ketika kekuatan baru ini mendekati atau bahkan melampaui kekuatan hegemon yang ada, sistem internasional memasuki fase transisi kekuasaan. Fase ini dianggap sangat berbahaya karena dapat memicu ketidakstabilan dan bahkan perang besar. Hal ini terjadi karena kekuatan baru yang bangkit sering kali tidak puas dengan status quo yang ditetapkan oleh hegemon lama, dan mereka berusaha untuk mengubah aturan sistem internasional agar lebih sesuai dengan kepentingan mereka.[14]

Teori Kebangkitan Kekuatan sangat relevan untuk memahami kebangkitan China sebagai kekuatan global dan implikasinya terhadap stabilitas internasional. China telah mengalami pertumbuhan ekonomi yang luar biasa selama beberapa dekade terakhir, dan kekuatan militernya juga meningkat secara signifikan. Hal ini telah menempatkan China pada posisi untuk menantang dominasi AS sebagai hegemon global. Namun, kebangkitan China juga memicu ketakutan di kalangan kekuatan-kekuatan lain, terutama AS. AS mungkin merasa bahwa kebangkitan China mengancam posisinya sebagai hegemon global, dan hal ini dapat memicu persaingan strategis antara kedua negara. Beberapa analis bahkan memperingatkan bahwa hubungan AS-China dapat terjebak dalam "Thucydides Trap," yang berpotensi memicu konflik besar.

METODOLOGI PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan tujuan utama memperoleh pemahaman yang mendalam mengenai isu yang dikaji. Pemilihan metode ini didasarkan pada kemampuannya dalam menyajikan data secara deskriptif, sehingga memungkinkan peneliti untuk menggali informasi secara lebih rinci dan dalam konteks yang lebih luas. Pendekatan yang diterapkan dalam penelitian ini adalah wawancara terfokus (focused interview), di mana peneliti berinteraksi secara langsung dan melakukan pertemuan tatap muka dengan informan untuk memperoleh data yang lebih kaya dan mendalam. Fokus utama dari penelitian ini

[12] Kugler, Jacek, and Tammen, Ronald L. (2012). *The Performance of Nations*. Lanham, MD: Rowman & Littlefield.
[13] Allison, Graham. (2017). *Destined for War: Can America and China Escape Thucydides's Trap?* Boston: Houghton Mifflin Harcourt.
[14] Tammen, Ronald L., et al. (2000). *Power Transitions: Strategies for the 21st Century*. New York: Chatham House Publishers.

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 2, No. 2 Tahun 2026 Hal. 176-193
e-ISSN: 3110-6048 DOI: 10.36859/dgsj.v2i2.5620

Article History:
Submitted:Feb 20, 2026
Accepted: Mar 21, 2026
Published: Apr 28, 2026

adalah untuk mengkaji Perkembangan Siber dan Dominasi Teknologi Militer China dalam Geopolitik di Kawasan.

Metode kualitatif memiliki karakteristik utama dalam penyajian data yang bersifat deskriptif-naratif, mencerminkan berbagai perspektif, gagasan, dan pendapat dari beragam sumber. Data yang diperoleh melalui wawancara kemudian diklasifikasikan berdasarkan relevansinya dengan pertanyaan penelitian menggunakan pendekatan interpretatif. Pendekatan ini bertujuan untuk memberikan pemahaman yang lebih mendalam dan sistematis mengenai subjek yang diteliti. Lebih lanjut, penelitian ini menerapkan pendekatan fenomenologi, yang memungkinkan peneliti untuk memahami realitas berdasarkan pengalaman subjektif para informan atau partisipan. Pendekatan ini memberikan wawasan tentang pengalaman mereka dalam tiga fase waktu yang berbeda: sebelum, selama, dan setelah fenomena yang menjadi fokus penelitian. Dengan demikian, fenomenologi membantu dalam menggambarkan pengalaman individu dalam konteks yang lebih komprehensif, termasuk bagaimana emosi, pemikiran, dan perspektif mereka berkembang seiring waktu.

Selain itu, metode kualitatif yang digunakan dalam penelitian ini melibatkan pengumpulan data empiris dari berbagai sumber, seperti pengalaman langsung, observasi lapangan, wawancara mendalam, serta dokumen dan arsip yang relevan dengan topik penelitian. Setelah data dikumpulkan, analisis dilakukan untuk menjawab pertanyaan-pertanyaan utama dalam penelitian ini. Selain wawancara, penelitian ini juga mengintegrasikan studi dokumentasi, observasi langsung, dan survei lapangan, yang bertujuan untuk memperkaya pemahaman terhadap isu yang dikaji. Wawancara dilakukan dengan narasumber yang memiliki keahlian dan wawasan mendalam mengenai topik penelitian, sehingga hasil penelitian dapat lebih akurat dan kredibel. Dengan demikian, penelitian ini diharapkan dapat memberikan pemahaman yang komprehensif dan mendalam mengenai Perkembangan Siber dan Dominasi Teknologi Militer China dalam Geopolitik di Kawasan.

PEMBAHASAN

Strategi Perang Siber yang Diterapkan oleh China dalam Upaya Meningkatkan Pengaruhnya di Kawasan Indo-Pasifik

Dalam dinamika geopolitik global, perkembangan teknologi siber telah menjadi salah satu faktor utama dalam membentuk kekuatan suatu negara. China, sebagai salah satu negara dengan pertumbuhan ekonomi dan militer yang pesat, telah mengadopsi strategi perang siber sebagai bagian integral dari upayanya untuk meningkatkan pengaruh di kawasan Indo-Pasifik. Dengan memanfaatkan keunggulan teknologi digital, China berusaha untuk memperkuat posisi strategisnya di tengah persaingan global yang semakin kompleks. Strategi perang siber yang diterapkan oleh China tidak hanya mencakup aspek pertahanan tetapi juga ofensif. Beijing telah membangun kapabilitas siber yang signifikan, mencakup operasi peretasan, kampanye disinformasi, serta pengembangan teknologi kecerdasan buatan yang

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 2, No. 2 Tahun 2026 Hal. 176-193
e-ISSN: 3110-6048 DOI: 10.36859/dgsj.v2i2.5620

Article History:
Submitted:Feb 20, 2026
Accepted: Mar 21, 2026
Published: Apr 28, 2026

berkontribusi pada superioritas informasi.[15] China memahami bahwa dalam era digital, dominasi informasi dapat menjadi senjata yang lebih efektif dibandingkan dengan kekuatan militer konvensional. Oleh karena itu, strategi perang siber yang dikembangkan berorientasi pada penguasaan infrastruktur digital, pengendalian narasi informasi, serta penggalangan pengaruh melalui berbagai platform digital.[16]

Dalam konteks Indo-Pasifik, strategi perang siber China diarahkan untuk mencapai beberapa tujuan utama.[34] Pertama, Beijing berupaya untuk meningkatkan kendali atas infrastruktur digital di negara-negara mitra dan pesaingnya. Ini mencakup investasi dalam teknologi jaringan 5G melalui perusahaan-perusahaan seperti Huawei dan ZTE, yang memungkinkan China untuk memiliki akses luas terhadap data dan sistem komunikasi di berbagai negara. Kedua, China menggunakan perang siber sebagai alat untuk mempengaruhi kebijakan dan opini publik di kawasan. Melalui propaganda digital, kampanye disinformasi, serta manipulasi media sosial, China berusaha membentuk persepsi yang menguntungkan bagi kepentingannya dan melemahkan posisi negara-negara yang dianggap sebagai ancaman. Ketiga, China mengembangkan strategi perang siber untuk meningkatkan efektivitas militernya dalam skenario konflik di masa depan. Dengan kemampuan perang elektronik, serangan siber terhadap infrastruktur kritis lawan, serta penggunaan kecerdasan buatan dalam pengambilan keputusan militer, China berupaya untuk menciptakan keunggulan taktis yang dapat memberikan efek strategis di kawasan. Hal ini sejalan dengan konsep "informatized warfare" yang dikembangkan oleh Tentara Pembebasan Rakyat (People's Liberation Army/PLA), di mana dominasi informasi menjadi elemen kunci dalam memenangkan peperangan modern.

Dalam beberapa tahun terakhir, berbagai insiden telah menunjukkan bagaimana China menerapkan strategi perang siber untuk meningkatkan pengaruhnya di Indo-Pasifik.[17] Beberapa negara seperti Australia, Jepang, dan India telah melaporkan adanya serangan siber yang diduga dilakukan oleh kelompok peretas yang memiliki keterkaitan dengan pemerintah China. Serangan-serangan ini sering kali menargetkan sektor-sektor kritis seperti pemerintahan, industri pertahanan, serta infrastruktur keuangan. Selain itu, China juga terlibat dalam kegiatan spionase siber yang bertujuan untuk mencuri informasi sensitif dari negara-negara pesaingnya. Di sisi lain, China juga memanfaatkan strategi perang siber dalam kerangka diplomasi digital.

Dengan meningkatkan kerja sama di bidang teknologi dan keamanan siber dengan negara-negara di kawasan Indo-Pasifik, China berusaha membangun ketergantungan yang dapat memperkuat posisinya sebagai pemimpin regional. Inisiatif seperti Digital Silk Road, yang merupakan bagian dari Belt and Road Initiative (BRI), menjadi salah satu sarana utama dalam ekspansi pengaruh siber China di kawasan.[36] Melalui proyek ini, China menyediakan

[15] Cheung, T. M. (2019). Forging China's Military Might: A New Framework for Assessing Innovation. Johns Hopkins University Press.

[16] Kania, E. B. (2017). Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power. Center for a New American Security. [34] Ibid.

[17] Rolland, N. (2017). China's Eurasian Century? Political and Strategic Implications of the Belt and Road Initiative. The National Bureau of Asian Research. [36] Ibid.

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 2, No. 2 Tahun 2026 Hal. 176-193
e-ISSN: 3110-6048 DOI: 10.36859/dgsj.v2i2.5620

Article History:
Submitted:Feb 20, 2026
Accepted: Mar 21, 2026
Published: Apr 28, 2026

infrastruktur digital, layanan cloud computing, serta teknologi kecerdasan buatan kepada negara-negara mitra, yang pada akhirnya memberikan Beijing akses yang lebih besar terhadap data dan sistem komunikasi di kawasan. Namun, strategi perang siber China tidak lepas dari tantangan dan resistensi. Negara-negara di kawasan Indo-Pasifik, terutama yang memiliki hubungan dekat dengan Amerika Serikat dan sekutu-sekutunya, telah mulai mengembangkan kebijakan untuk mengurangi ketergantungan pada teknologi China. Langkahlangkah seperti pelarangan penggunaan peralatan jaringan dari perusahaan China, peningkatan kerja sama keamanan siber dengan negara-negara Barat, serta penguatan regulasi terkait perlindungan data menjadi bagian dari upaya untuk mengimbangi pengaruh China dalam ranah siber.

Secara keseluruhan, strategi perang siber yang diterapkan oleh China mencerminkan pendekatan multidimensional dalam upaya meningkatkan pengaruhnya di Indo-Pasifik. Dengan mengkombinasikan aspek teknologi, ekonomi, dan militer, China telah menciptakan ekosistem siber yang mampu memberikan keunggulan strategis di kawasan. Bab ini akan membahas lebih lanjut mengenai berbagai elemen dari strategi perang siber China, termasuk analisis terhadap dampaknya terhadap dinamika geopolitik regional, serta respons yang diambil oleh negara-negara di kawasan untuk menghadapi ancaman siber dari Beijing. Dengan pemahaman yang lebih mendalam mengenai strategi ini, kita dapat melihat bagaimana perang siber menjadi elemen kunci dalam persaingan geopolitik kontemporer dan bagaimana negara-negara di kawasan Indo-Pasifik dapat menavigasi tantangan yang ditimbulkan oleh perkembangan ini.

Strategi Perang Siber Yang Diterapkan Oleh China Dalam Upaya Meningkatkan Pengaruhnya Di Kawasan Indo-Pasifik

Guna memahami strategi perang siber yang diterapkan oleh China dalam meningkatkan pengaruhnya di kawasan Indo-Pasifik, perlu melihatnya dari berbagai perspektif teoritis yang relevan dalam studi hubungan internasional. Pendekatan realisme, Teori Kebangkitan Kekuatan (*Power Transition Theory*), serta konsep hegemoni merupakan pendekatan dan teori yang peneliti gunakan untuk memberikan landasan yang kuat dalam menganalisis motivasi dan implikasi dari strategi siber China.

Realisme, sebagai salah satu teori utama dalam hubungan internasional, menekankan pada kepentingan nasional dan persaingan antarnegara dalam mencapai dominasi. Hans Morgenthau berargumen bahwa negara-negara bertindak berdasarkan kepentingan nasional mereka yang sering kali berkaitan dengan peningkatan kekuatan dan keamanan. Dalam konteks perang siber, strategi China dapat dipahami sebagai upaya untuk memperkuat posisinya dalam lanskap geopolitik serta mengurangi potensi ancaman dari negara-negara pesaing, terutama Amerika Serikat dan sekutunya di kawasan Indo-Pasifik. Perang siber menjadi alat yang efektif bagi China untuk memperoleh keunggulan tanpa harus terlibat dalam konflik militer konvensional. Dengan mengembangkan kapabilitas siber yang semakin canggih, China dapat mengakses informasi strategis, melemahkan infrastruktur lawan, serta membentuk opini publik di berbagai negara untuk kepentingannya.

Dalam perspektif Teori Kebangkitan Kekuatan yang dikembangkan oleh A.F.K. Organski, perubahan keseimbangan kekuatan global sering kali membawa ketegangan dan

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 2, No. 2 Tahun 2026 Hal. 176-193
e-ISSN: 3110-6048 DOI: 10.36859/dgsj.v2i2.5620

Article History:
Submitted:Feb 20, 2026
Accepted: Mar 21, 2026
Published: Apr 28, 2026

potensi konflik antara negara yang sedang bangkit dengan negara yang berusaha mempertahankan status quo. Dalam konteks ini, China adalah kekuatan yang sedang menanjak dan berusaha menantang dominasi Amerika Serikat di kawasan Indo-Pasifik. Perang siber menjadi instrumen penting dalam mempercepat transisi kekuatan ini dengan cara merusak keunggulan teknologi dan ekonomi lawan. Melalui operasi peretasan dan pencurian data dari berbagai perusahaan serta institusi pemerintah, China memperoleh keuntungan strategis yang signifikan, mempercepat kebangkitannya sebagai kekuatan global. Selain itu, disinformasi dan propaganda digital digunakan untuk melemahkan legitimasi negara-negara rival serta membangun narasi yang menguntungkan bagi kepentingan geopolitik China.

Konsep hegemoni dalam hubungan internasional juga memberikan wawasan penting dalam memahami bagaimana China menggunakan perang siber sebagai bagian dari strategi globalnya. Robert Keohane berpendapat bahwa hegemoni dapat beroperasi melalui kendali terhadap institusi dan aturan internasional. Dalam konteks perang siber, China berupaya menciptakan hegemoni digital dengan mengendalikan infrastruktur komunikasi global melalui inisiatif seperti Digital Silk Road serta dominasi perusahaan teknologi seperti Huawei dan Alibaba. Upaya ini memungkinkan China untuk mempengaruhi standar teknologi global, memastikan bahwa negara-negara mitranya bergantung pada teknologi China, dan secara tidak langsung meningkatkan kontrolnya atas arus informasi. Selain itu, perang siber juga digunakan untuk menekan perlawanan terhadap dominasi China di kawasan, baik melalui serangan terhadap infrastruktur digital lawan maupun kampanye propaganda yang bertujuan membentuk citra positif bagi kepemimpinan Beijing.

Dari analisis terhadap strategi perang siber yang diterapkan oleh China, tampak bahwa pendekatan ini memiliki beberapa implikasi yang signifikan bagi keamanan kawasan Indo-Pasifik. Salah satu dampak utama adalah meningkatnya ancaman terhadap keamanan siber di kawasan. China secara aktif melakukan operasi peretasan terhadap berbagai institusi pemerintah dan sektor swasta di negara-negara Indo-Pasifik, yang mencakup pencurian data strategis, sabotase infrastruktur digital, serta pengumpulan informasi intelijen. Dalam beberapa kasus, serangan siber yang dilakukan China telah menyebabkan gangguan terhadap jaringan komunikasi dan sistem kritis di negara-negara yang dianggap sebagai ancaman terhadap kepentingannya.

Selain itu, perang siber juga berpengaruh terhadap stabilitas politik dan ekonomi di kawasan. Dengan memanfaatkan teknologi digital, China mampu memanipulasi opini publik melalui kampanye disinformasi dan propaganda daring. Strategi ini digunakan untuk mendukung kandidat politik atau kelompok yang proChina di berbagai negara serta melemahkan oposisi yang menentang kebijakan Beijing. Dampaknya tidak hanya terbatas pada aspek politik, tetapi juga mencakup sektor ekonomi, terutama dalam persaingan bisnis global di industri teknologi dan manufaktur. Perusahaan-perusahaan China yang didukung oleh pemerintah memiliki akses ke informasi dan teknologi yang diperoleh melalui operasi peretasan, memberikan mereka keunggulan dalam persaingan global.

Namun, strategi perang siber China juga menimbulkan respons yang semakin kuat dari negara-negara yang merasa terancam oleh ekspansi digital Beijing. Amerika Serikat, Australia, Jepang, dan India, misalnya, telah memperkuat kerja sama dalam bidang keamanan

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 2, No. 2 Tahun 2026 Hal. 176-193
e-ISSN: 3110-6048 DOI: 10.36859/dgsj.v2i2.5620

Article History:
Submitted:Feb 20, 2026
Accepted: Mar 21, 2026
Published: Apr 28, 2026

siber melalui inisiatif seperti Quad dan aliansi teknologi. Negara-negara ini juga berusaha mengembangkan alternatif terhadap infrastruktur digital China untuk mengurangi ketergantungan pada teknologi yang dikendalikan Beijing. Respons ini menunjukkan bahwa meskipun perang siber memberikan keuntungan bagi China, ia juga memicu perlawanan dari negaranegara pesaing, yang berupaya untuk membatasi pengaruhnya dalam lanskap digital global.

Dinamika ini menunjukkan bagaimana perang siber menjadi elemen penting dalam perubahan keseimbangan kekuatan di Indo-Pasifik. China menggunakan strategi ini untuk menekan dominasi Amerika Serikat dan membangun pengaruhnya di negara-negara berkembang melalui diplomasi digital dan ekonomi. Namun, pendekatan agresif dalam perang siber juga berisiko memicu eskalasi konflik dan memperburuk hubungan internasional. Dalam jangka panjang, keberhasilan strategi ini akan sangat bergantung pada bagaimana China menavigasi resistensi dari negara-negara pesaing serta menjaga stabilitas dalam sistem internasional. Dengan demikian, perang siber tidak hanya menjadi alat untuk memperkuat dominasi China, tetapi juga faktor yang dapat menentukan arah keamanan dan geopolitik kawasan Indo-Pasifik di masa depan.

Implikasi Dominasi Teknologi Militer China Terhadap Stabilitas Keamanan Di Kawasan Indo-Pasifik

Dominasi teknologi militer China di kawasan Indo-Pasifik memiliki dampak yang signifikan terhadap stabilitas keamanan regional. Untuk memahami implikasi dari fenomena ini, tiga pendekatan teoretis digunakan oleh peneliti sebagai pisau analisa, yaitu Teori *Security Dilemma*, Konsep Hegemoni, dan Teori Keamanan Kompleks (*Security Complex Theory*). Pendekatan ini memberikan gambaran yang lebih komprehensif tentang bagaimana dominasi militer China membentuk dinamika keamanan di kawasan.

Teori *Security Dilemma* yang dikemukakan oleh John Herz dan Robert Jervis menjelaskan bagaimana upaya suatu negara untuk meningkatkan keamanannya justru dapat memicu ketidakstabilan. Dalam konteks ini, modernisasi teknologi militer China—termasuk pengembangan kecerdasan buatan dalam sistem persenjataan, peningkatan kapabilitas siber, serta pembangunan sistem persenjataan hipersonik—dapat dilihat sebagai langkah defensif oleh Beijing. Namun, negaranegara lain di kawasan seperti Jepang, India, Australia, dan anggota ASEAN melihatnya sebagai ancaman potensial yang memicu respons strategis berupa peningkatan aliansi keamanan, peningkatan anggaran pertahanan, serta pengembangan teknologi militer mereka sendiri. Situasi ini menciptakan spiral ketidakpercayaan yang berujung pada perlombaan senjata di kawasan, yang pada akhirnya memperbesar risiko konflik yang tidak disengaja.

Sementara itu, Konsep Hegemoni yang dikembangkan oleh Antonio Gramsci dan diperluas oleh Robert Keohane dapat digunakan untuk memahami bagaimana dominasi militer China berperan dalam mengkonsolidasikan pengaruhnya di kawasan. Hegemoni tidak hanya terbentuk melalui kekuatan militer, tetapi juga melalui kontrol terhadap ekonomi dan teknologi. China memanfaatkan dominasi teknologinya untuk memperkuat posisi hegemoniknya di Indo-Pasifik, antara lain dengan membangun ketergantungan negara-negara lain terhadap sistem persenjataan dan infrastruktur teknologi yang mereka

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 2, No. 2 Tahun 2026 Hal. 176-193
e-ISSN: 3110-6048 DOI: 10.36859/dgsj.v2i2.5620

Article History:
Submitted:Feb 20, 2026
Accepted: Mar 21, 2026
Published: Apr 28, 2026

kembangkan. Misalnya, proyek Digital Silk Road dalam inisiatif Belt and Road Initiative (BRI) tidak hanya berfungsi sebagai proyek ekonomi, tetapi juga sebagai alat untuk mengintegrasikan sistem keamanan siber negara-negara mitra dengan infrastruktur teknologi yang dikuasai China. Dengan demikian, China dapat menciptakan ekosistem strategis di mana negara-negara mitranya sulit melepaskan diri dari pengaruh Beijing.

Selain itu, Teori Keamanan Kompleks (*Security Complex Theory*) yang diperkenalkan oleh Barry Buzan memberikan perspektif mengenai bagaimana keamanan suatu negara tidak dapat dipisahkan dari keamanan negara lain di sekitarnya. Dalam konteks Indo-Pasifik, peningkatan teknologi militer China tidak hanya berimplikasi pada hubungan bilateral dengan Amerika Serikat, tetapi juga berdampak pada konfigurasi keamanan kawasan secara keseluruhan. Negaranegara di kawasan ini semakin melihat keamanan mereka sebagai bagian dari sistem yang saling terkait, sehingga muncul pola interaksi keamanan yang lebih kompleks. Aliansi seperti Quad (AS, India, Jepang, Australia) dan AUKUS (AS, Inggris, Australia) dapat dilihat sebagai respons terhadap dominasi militer China, yang menciptakan blok-blok keamanan yang berpotensi meningkatkan ketegangan geopolitik.

Dalam praktiknya, dominasi teknologi militer China menciptakan berbagai implikasi yang memengaruhi stabilitas kawasan Indo-Pasifik. Salah satunya adalah peningkatan aktivitas militer di Laut China Selatan, di mana China mengadopsi teknologi mutakhir seperti kecerdasan buatan dan sistem pengawasan berbasis drone untuk memperkuat klaim teritorialnya. Hal ini menimbulkan reaksi keras dari negara-negara lain yang juga memiliki klaim di wilayah tersebut, seperti Filipina, Vietnam, dan Malaysia. Selain itu, peningkatan kemampuan siber China menimbulkan ancaman terhadap infrastruktur kritis negara-negara tetangganya, meningkatkan kekhawatiran akan kemungkinan perang siber sebagai bagian dari strategi konflik asimetris di masa depan. Di sisi lain, dominasi teknologi militer China juga berkontribusi terhadap pergeseran keseimbangan kekuatan global.

Amerika Serikat, yang selama ini menjadi aktor dominan dalam sistem keamanan Indo-Pasifik, mulai menghadapi tantangan dari Beijing yang semakin berani menantang supremasi militer Washington di kawasan. Pergeseran ini tidak hanya berdampak pada dinamika militer, tetapi juga pada stabilitas ekonomi dan diplomasi di Indo-Pasifik. Negara-negara yang berada di bawah tekanan dari kedua kekuatan ini harus menavigasi kebijakan luar negeri mereka dengan hati-hati agar tidak terjebak dalam konflik kepentingan antara dua kekuatan besar ini.

Dalam jangka panjang, keberlanjutan dominasi teknologi militer China kemungkinan besar akan mempercepat multipolaritas di kawasan Indo-Pasifik, dengan lebih banyak negara yang mencoba mengembangkan kapabilitas militer dan sibernya sendiri untuk mengimbangi pengaruh Beijing. Namun, tanpa adanya mekanisme kepercayaan dan dialog strategis yang efektif, risiko eskalasi konflik akan tetap tinggi. Oleh karena itu, pendekatan diplomatik yang berorientasi pada de-eskalasi perlu dikembangkan untuk mencegah ketegangan yang dapat berujung pada konflik berskala besar. Dengan memahami dinamika ini melalui perspektif teori hubungan internasional, dapat diperoleh wawasan yang lebih dalam mengenai bagaimana stabilitas keamanan di kawasan Indo-Pasifik dapat dikelola dalam menghadapi dominasi teknologi militer China.

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 2, No. 2 Tahun 2026 Hal. 176-193
e-ISSN: 3110-6048 DOI: 10.36859/dgsj.v2i2.5620

Article History:
Submitted:Feb 20, 2026
Accepted: Mar 21, 2026
Published: Apr 28, 2026

KESIMPULAN

China menerapkan strategi perang siber yang terintegrasi dengan pendekatan militer dan geopolitik untuk memperkuat pengaruhnya di kawasan Indo-Pasifik. Strategi ini mencakup operasi peretasan, spionase siber, disinformasi, serta manipulasi media digital guna melemahkan lawan dan membentuk narasi yang menguntungkan bagi Beijing. Dengan mengembangkan kapabilitas siber yang canggih, China tidak hanya mampu mencuri data strategis dari negara-negara pesaing, tetapi juga memanfaatkan teknologi digital untuk memperkuat posisi hegemoniknya melalui inisiatif seperti Digital Silk Road dalam Belt and Road Initiative (BRI). Pendekatan ini memungkinkan China untuk memperluas pengaruh politik, ekonomi, dan keamanannya tanpa harus terlibat dalam konfrontasi militer langsung.

Lebih lanjut, dominasi teknologi militer China berdampak signifikan terhadap stabilitas kawasan Indo-Pasifik. Dari perspektif Security Dilemma, modernisasi militer dan siber China memicu respons strategis dari negara-negara lain, yang meningkatkan perlombaan senjata dan memperburuk ketegangan geopolitik. Dengan menggunakan konsep hegemoni, China menciptakan ketergantungan negara-negara mitra pada teknologi dan sistem pertahanannya, yang memperkuat posisinya di kawasan. Sementara itu, Teori Keamanan Kompleks menunjukkan bahwa respons dari negara-negara seperti Amerika Serikat, Jepang, India, dan Australia terhadap kebangkitan militer China telah membentuk blok-blok keamanan baru seperti Quad dan AUKUS, yang berpotensi meningkatkan fragmentasi kawasan. Jika tidak dikelola dengan baik melalui mekanisme diplomasi dan kerja sama keamanan yang efektif, dominasi teknologi militer China dapat meningkatkan risiko konflik serta mengganggu stabilitas jangka panjang di Indo-Pasifik.

DAFTAR PUSTAKA

Allison, Graham. (2017). Destined for War: Can America and China Escape Thucydides's Trap? Boston: Houghton Mifflin Harcourt.

Australian Strategic Policy Institute (ASPI). (2020). China’s Cyber Influence in Australia’s Democracy. ASPI Reports.

Buzan, B. (1991). People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era. Harvester Wheatsheaf.

Buzan, B., & Waever, O. (2003). Regions and Powers: The Structure of International Security. Cambridge: Cambridge University Press.

Center for Strategic and International Studies (CSIS). (2021). China’s Cyber Capabilities and Military Strategy. CSIS Reports.

Cheung, T. M. (2019). Forging China's Military Might: A New Framework for Assessing Innovation. Johns Hopkins University Press.

China People’s Liberation Army, 2004. China White Paper. Diakses melalui : http://www.china.org.cn/e-white/20041227/III.htm#5

Congressional Research Service. (2023). China’s Military Modernization: Implications for U.S. Defense. Washington, D.C.: CRS.

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 2, No. 2 Tahun 2026 Hal. 176-193
e-ISSN: 3110-6048 DOI: 10.36859/dgsj.v2i2.5620

Article History:
Submitted:Feb 20, 2026
Accepted: Mar 21, 2026
Published: Apr 28, 2026

Cordesman, A. H. (2020). China's Military Modernization: Force Development and Strategic Capabilities. CSIS.

CSIRT, 2025. Serangan Siber China: Ancaman Global pada AS dan Taiwan. Diakses melalui: https://csirt.or.id/berita/serangan-siber-china-as-taiwan

Erickson, A. S., & Kennedy, C. M. (2022). China's Maritime Strategy: The Role of the People's Liberation Army Navy. Naval War College Review.

Fearon, J. D. (1995). Rationalist Explanations for War. International Organization, 49(3), 379-414.

Federal Bureau of Investigation (FBI). (2016). OPM Data Breach: China's Cyber Espionage Activities. FBI Reports.

Forbes, 2023. Spotlight On APT10. Diakses melalui : https://www.forbes.com/sites/emilsayegh/2023/02/21/spotlight-on-apt10/

Fung, C. J. (2020). China's Cyber Power: Strategic Objectives and Policy Implications. International Affairs.

Gautam Chhabara, 2020. How Huawei came to rule the 5G World?. Diakses melalui: https://www.linkedin.com/pulse/how-huawei-came-rule-5gworld-gautam-chhabra

Gramsci, A. (1971). Selections from the Prison Notebooks. New York: International Publishers.

Heath, T. (2018). China's Cyber Warfare and Military Strategy. RAND Corporation.

Herz, J. H. (1950). Political Realism and Political Idealism: A Study in Theories and Realities. Chicago: University of Chicago Press.

Hobbes, T. (1651). Leviathan. London: Andrew Crooke.

Indo-Pacific Forum Defense, 2024. Fake news, nonexistent journalists part of Beijing's information manipulation scheme. Diakses melalui: https://ipdefenseforum.com/2024/10/fake-news-nonexistent-journalistspart-of-beijings-information-manipulation-scheme/

J.C Johari 1985 dalam Teuku May Rudy, Administrasi dan Organisasi Internasional (Bandung: PT Refika Aditama, 2005), hlm. 71.

Jervis, R. (1978). Cooperation Under the Security Dilemma. World Politics, 30(2), 167-214.

Kania, E. B. (2017). Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power. Center for a New American Security.

Kania, E. B. (2019). China's Strategic Investment in AI and 5G. Center for a New American Security.

Kania, E. B. (2021). AI and the Future of Warfare: China's Strategic Perspective. The Diplomat.

Kaplan, R. D. (2014). Asia's Cauldron: The South China Sea and the End of a Stable Pacific. Random House.

Keohane, R. O. (1984). After Hegemony: Cooperation and Discord in the World Political Economy. Princeton: Princeton University Press.

Kugler, Jacek, and Tammen, Ronald L. (2012). The Performance of Nations. Lanham, MD: Rowman & Littlefield.

Lee, K.-F. (2018). AI Superpowers: China, Silicon Valley, and the New World Order. Houghton Mifflin Harcourt.

DIPLOMACY AND GLOBAL SECURITY JOURNAL
Jurnal Mahasiswa Magister Hubungan Internasional
Vol. 2, No. 2 Tahun 2026 Hal. 176-193
e-ISSN: 3110-6048 DOI: 10.36859/dgsj.v2i2.5620

Article History:
Submitted:Feb 20, 2026
Accepted: Mar 21, 2026
Published: Apr 28, 2026

Lyu Jinghua, 2022. What Are China's Cyber Capabilities and Intentions?. Diakses melalui : https://carnegieendowment.org/posts/2019/04/what-arechinas-cyber-capabilities-and-intentions?lang=en

Machiavelli, N. (1532). The Prince. Florence: Antonio Blado d'Asola.

Mandiant. (2013). APT1: Exposing One of China's Cyber Espionage Units. FireEye.

Mearsheimer, J. J. (2001). The Tragedy of Great Power Politics. New York: W. W. Norton & Company.

Miles dan A. Michael Huberman, 1992.Hal: 15-17

Mix mode, 2023. APT 1, COMMENT PANDA – PLA Unit 61398, CHINA. Diakses elalui: https://mixmode.ai/threat-intelligence-research/apt-1comment-panda-pla-unit-61398china/#___APT_1_COMMENT_PANDA__PLA_Unit_61398_CHINA_

Morgenthau, H. J. (1948). Politics Among Nations: The Struggle for Power and Peace. New York: Alfred A. Knopf.

Nathaniel Richmond, 2019. Operation Cloud Hopper Case Study. Diakses melalui: https://insights.sei.cmu.edu/blog/operation-cloud-hopper-casestudy/

Organski, A.F.K. (1958). World Politics. New York: Knopf.

Peter Harrell, 2025. Managing the Risks of China's Access to U.S. Data and Control of Software and Connected Technology. Diakses melalui : https://carnegieendowment.org/research/2025/01/managing-the-risks-ofchinas-access-to-us-data-and-control-of-software-and-connectedtechnology?lang=en

Publikasi Ilmiah UNWAHAS. (2023). Analisis Strategi Keamanan Siber China di Kawasan Indo-Pasifik. Diakses melalui: https://publikasiilmiah.unwahas.ac.id

Rolland, N. (2017). China's Eurasian Century? Political and Strategic Implications of the Belt and Road Initiative. The National Bureau of Asian Research.

Sanger, D. E. (2018). The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age. Crown Publishing Group

Segal, A. (2017). The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age. PublicAffairs.

Steven Feldstein, 2022. Disentangling The Digital Battlefield: How the Internet Has Changed War. Diakses melalui : https://warontherocks.com/2022/12/disentangling-the-digital-battlefieldhow-the-internet-has-changed-war/

Sugiyono. 2004. Metode Penelitian. Bandung: Alfabeta.

Sugiyono. 2013. Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Bandung: CV. Alfabeta.

Tammen, Ronald L., et al. (2000). Power Transitions: Strategies for the 21st Century. New York: Chatham House Publishers.

Tempo, 2014. Penyusup Rahasia di Sudut Pudong. Diakses melalui: https://www.tempo.co/internasional/penyusup-rahasia-di-sudut-pudong-921684

UNAV. (2023). Chinese Cyber Warfare in the Indo-Pacific. University of Navarra. Diakses melalui : https://www.unav.edu/web/global-affairs

Universidad de Navarra, 2023. Chinese Cyber Warfare in the Indo-Pacific: An analysis of means, targets, and solutions. Diakses melalui : https://www.unav.edu/web/global-affairs/chinese-cyber-warfare-in-theindo-pacific

DIPLOMACY AND GLOBAL SECURITY JOURNAL **Jurnal Mahasiswa Magister Hubungan Internasional** **Vol. 2, No. 2 Tahun 2026 Hal. 176-193** **e-ISSN: 3110-6048 DOI: 10.36859/dgsj.v2i2.5620**	Article History: *Submitted:Feb 20, 2026* *Accepted: Mar 21, 2026* *Published: Apr 28, 2026*

US Department of justice, 2014. U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage. Diakses melalui: https://www.justice.gov/archives/opa/pr/us-charges-five-chinesemilitary-hackers-cyber-espionage-against-us-corporations-and-labor

Waltz, K. (1979). Theory of International Politics. Reading, MA: Addison-Wesley.

Wired, 2016. Inside the Cyberattack That Shocked the US Government. Diakses melalui: https://www.wired.com/2016/10/inside-cyberattack-shocked-usgovernment/

Zhang, D. (2021). China's Cybersecurity Law: A Comprehensive Analysis. Journal of Cybersecurity and Privacy.