Aurelia: Jurnal Penelitian dan Pengabdian Masyarakat Indonesia
E-ISSN: 2964-2493 P-ISSN: 2962-0430
Vol. 4 No. 2 Juli 2025

Ancaman Perang Siber China terhadap Indonesia: Analisis Strategi, Dampak, dan Respons Kebijakan

Keio Ariel[1] Suhirwan[2] Ahmad G Dohamid[3]
Universitas Pertahanan Republik Indonesia[1,2,3]
Email: keiriel19@gmail.com[1] suhirwan@idu.ac.id[2] ahmaddohamid@gmail.com[3]

Abstrak

Studi ini mengkaji karakteristik, strategi, dan dampak perang siber Tiongkok terhadap Indonesia, serta respons kebijakan dan tantangan Indonesia dalam keamanan siber. Memanfaatkan pendekatan kualitatif dengan studi kasus dan tinjauan literatur, penelitian ini menganalisis pola serangan siber Tiongkok, target, dan motivasinya. Temuan mengungkapkan bahwa Tiongkok menggunakan teknik canggih seperti Advanced Persistent Threats (APT) dan spear-phishing, yang menargetkan lembaga pemerintah, infrastruktur penting, dan perusahaan strategis di Indonesia. Dampaknya termasuk kerentanan dalam infrastruktur penting, pelanggaran data sensitif, dan gangguan ekonomi. Meskipun Indonesia telah mengambil langkah-langkah untuk meningkatkan pertahanan sibernya melalui kerangka hukum, pengembangan kemampuan, dan kerja sama internasional, kesenjangan yang signifikan tetap ada dalam teknologi, sumber daya manusia, dan koordinasi antar-lembaga. Studi ini menerapkan teori Pertahanan Nasional, Perang Asimetris, Pencegahan Siber, dan Keamanan Siber untuk memberikan pemahaman yang komprehensif tentang dinamika kompleks yang terlibat. Rekomendasi tersebut meliputi peningkatan investasi dalam teknologi dan infrastruktur keamanan siber, pengembangan sumber daya manusia, penguatan kerangka hukum, meningkatkan koordinasi antar pemangku kepentingan.
Kata Kunci: Pertahanan Nasional, Keamanan Nasional, Peperangan Asimetris, Pencegahan Siber, Keamanan Siber

Abstract

This study examines the characteristics, strategies, and impacts of China's cyber warfare against Indonesia, as well as Indonesia's policy responses and challenges in cybersecurity. Utilizing a qualitative approach with case studies and literature review, the research analyzes the patterns of Chinese cyber attacks, their targets, and motivations. Findings reveal that China employs sophisticated techniques such as Advanced Persistent Threats (APTs) and spear-phishing, targeting government institutions, critical infrastructure, and strategic companies in Indonesia. The impacts include vulnerabilities in critical infrastructure, sensitive data breaches, and economic disruptions. While Indonesia has taken steps to enhance its cyber defense through legal frameworks, capability building, and international cooperation, significant gaps remain in technology, human resources, and inter-agency coordination. The study applies theories of National Defense, Asymmetric Warfare, Cyber Deterrence, and Cybersecurity to provide a comprehensive understanding of the complex dynamics involved. Recommendations include increased investment in cybersecurity technology and infrastructure, human resource development, strengthening legal frameworks, improving coordination among stakeholders, and enhancing cyber diplomacy. This research contributes to the growing literature on cyber warfare in Southeast Asia and provides valuable insights for policymakers in formulating effective national cybersecurity strategies.
Keywords: *National Defense, National Security, Asymmetric Warfare, Cyber Deterrence, Cyber Security*

PENDAHULUAN

Dalam era digital yang semakin terhubung, perang siber telah menjadi dimensi baru dalam konflik geopolitik global. China, sebagai kekuatan ekonomi dan teknologi yang berkembang pesat, telah muncul sebagai aktor utama dalam arena perang siber, dengan kapabilitas dan ambisi yang signifikan (Ball, 2011). Indonesia, sebagai negara dengan ekonomi terbesar di Asia Tenggara dan lokasi strategis, telah menjadi target utama operasi siber China di kawasan ini (Hjortdal, 2011). Menurut laporan dari *Universidad de Navarra* (2023), Indonesia merupakan negara kedua yang paling sering menjadi sasaran serangan siber dari China di kawasan Indo-Pasifik. Pada tahun 2021, terjadi peretasan terhadap sepuluh kementerian pemerintah, lembaga militer, dan bahkan layanan intelijen Indonesia oleh kelompok *cyber-espionage* China yang dikenal sebagai *Mustang Panda*. Insiden ini menunjukkan tingkat sophistikasi dan agresivitas operasi siber China terhadap Indonesia. Motivasi di balik serangan siber China terhadap Indonesia bersifat multifaset. Kolton (2017) berpendapat bahwa tujuan utama China adalah untuk mendapatkan keunggulan geopolitik dan ekonomi melalui pencurian data sensitif dan intelijen. Selain itu, upaya China untuk memperluas pengaruhnya di kawasan Indo-Pasifik, termasuk melalui inisiatif *Belt and Road*, juga memainkan peran penting dalam strategi perang sibernya (Universidad de Navarra, 2023).

Saat ini, Indonesia menghadapi ancaman siber yang semakin intensif dan canggih dari China. Infrastruktur digital Indonesia, termasuk sistem pemerintahan, militer, dan ekonomi, menjadi sasaran serangan yang bertujuan untuk mencuri data sensitif, melakukan espionase, dan potensial sabotase (Putra et al., 2020). Meskipun pemerintah Indonesia telah mulai meningkatkan kapabilitas pertahanan sibernya, masih terdapat kesenjangan signifikan dalam hal teknologi, sumber daya manusia, dan kerangka hukum yang komprehensif untuk menghadapi ancaman ini (Rizal & Yani, 2016). Idealnya, Indonesia harus memiliki sistem pertahanan siber yang tangguh dan komprehensif, mampu mendeteksi, mencegah, dan merespons serangan siber dengan efektif. Hal ini mencakup infrastruktur teknologi yang canggih, tenaga ahli yang memadai, kerangka hukum yang kuat, dan kerjasama internasional yang aktif dalam bidang keamanan siber. Indonesia juga perlu mengembangkan strategi *deterrence* siber yang efektif untuk mencegah serangan di masa depan (Sari, 2019). Terdapat kesenjangan yang signifikan antara kondisi saat ini dan yang diharapkan dalam konteks keamanan siber Indonesia menghadapi ancaman dari China. Beberapa gap utama meliputi: 1) Kesenjangan teknologi karena Indonesia masih tertinggal dalam hal teknologi keamanan siber dibandingkan dengan China (Putra et al., 2020); 2) Kekurangan sumber daya manusia: Terdapat kelangkaan tenaga ahli keamanan siber di Indonesia (Rizal & Yani, 2016); 3) Kelemahan kerangka hukum: Indonesia belum memiliki kerangka hukum yang komprehensif untuk mengatur dan merespons ancaman siber (Sari, 2019);4) Kurangnya koordinasi: Masih terdapat tantangan dalam koordinasi antar lembaga pemerintah dan sektor swasta dalam menghadapi ancaman siber (Putra et al., 2020); 5) Keterbatasan kerjasama internasional: Indonesia perlu meningkatkan partisipasi dan kolaborasinya dalam forum keamanan siber internasional (Rizal & Yani, 2016).

Penulisan makalah ini bertujuan untuk menganalisis secara komprehensif karakteristik, strategi, dan dampak perang siber China terhadap Indonesia. Selain itu, studi ini juga akan mengevaluasi respons kebijakan Indonesia dan mengidentifikasi area-area yang memerlukan peningkatan dalam menghadapi ancaman siber yang

berkembang. Dengan memahami dinamika ini, diharapkan dapat memberikan wawasan berharga bagi pembuat kebijakan, praktisi keamanan, dan akademisi dalam menghadapi tantangan keamanan siber di era kontemporer. Rumusan Masalah: Bagaimana karakteristik dan strategi perang siber China terhadap Indonesia, serta apa dampaknya terhadap keamanan nasional dan infrastruktur kritis Indonesia? Sejauh mana efektivitas respons kebijakan dan upaya pertahanan siber Indonesia dalam menghadapi ancaman siber dari China? Apa kesenjangan dan tantangan utama yang dihadapi Indonesia dalam mengembangkan kapabilitas pertahanan siber yang tangguh terhadap ancaman dari China? Tujuan Penelitian: Menganalisis dan mengidentifikasi pola serangan siber China terhadap Indonesia, termasuk target, metode, dan motivasi di balik serangan tersebut. Mengevaluasi kebijakan dan strategi pertahanan siber Indonesia saat ini, serta mengukur efektivitasnya dalam menangkal dan merespons ancaman siber dari China. Mengidentifikasi kesenjangan dalam kapabilitas pertahanan siber Indonesia dan merumuskan rekomendasi untuk meningkatkan ketahanan siber nasional terhadap ancaman dari China. Manfaat Penelitian: Kontribusi Akademis: Penelitian ini akan memperkaya literatur tentang perang siber di kawasan Asia Tenggara, khususnya dalam konteks hubungan China- Indonesia. Hal ini akan memberikan dasar teoritis dan empiris untuk studi lebih lanjut tentang dinamika keamanan siber regional. Implikasi Kebijakan: Hasil penelitian ini dapat menjadi masukan berharga bagi pembuat kebijakan di Indonesia dalam merumuskan strategi keamanan siber nasional yang lebih efektif dan responsif terhadap ancaman dari China. Rekomendasi yang dihasilkan dapat membantu dalam pengembangan kebijakan dan alokasi sumber daya yang lebih tepat sasaran. Peningkatan Kesadaran: Penelitian ini akan meningkatkan pemahaman dan kesadaran di kalangan pemerintah, sektor swasta, dan masyarakat umum tentang pentingnya keamanan siber dalam menghadapi ancaman dari negara- negara dengan kapabilitas siber yang maju seperti China. Hal ini dapat mendorong investasi yang lebih besar dalam pendidikan, pelatihan, dan pengembangan infrastruktur keamanan siber di Indonesia.

Tinjauan Pustaka

Teori Pertahanan Nasional (*National Defense Theory*) dari Barry Buzan (1991) digunakan sebagai kerangka utama untuk memahami aspek-aspek keamanan nasional dalam konteks ancaman siber. Baldwin (1997) menjelaskan bahwa konsep keamanan telah terlalu lama didominasi oleh perspektif negara-sentris dan militer-sentris. Kita perlu memperluas pemahaman kita tentang keamanan untuk mencakup ancaman non- tradisional. Senada dengan itu, Buzan (1991) menyatakan bahwa keamanan nasional harus dipahami dalam konteks yang lebih luas, melampaui dimensi militer tradisional untuk mencakup aspek politik, ekonomi, sosial, dan lingkungan. Teori ini menekankan pentingnya memahami keamanan sebagai konsep multidimensi yang mencakup aspek militer, politik, ekonomi, sosial, dan lingkungan. Konsep Peperangan Asimetris dari Andrew Mack (1975) diaplikasikan untuk menganalisis dinamika perang siber antara China dan Indonesia. Teori ini membantu menjelaskan bagaimana aktor dengan kapabilitas yang berbeda (dalam hal ini, China dan Indonesia) terlibat dalam konflik, dan bagaimana pihak yang lebih lemah dapat menghadapi pihak yang lebih kuat. Arreguin-Toft (2001) menambahkan perspektif penting bahwa hasil konflik asimetris sering ditentukan oleh interaksi strategis daripada perbandingan kekuatan yang sederhana. Ketika aktor yang lebih lemah menggunakan strategi yang berlawanan dengan lawannya, peluang mereka

untuk menang meningkat secara signifikan. Teori *Deterrence* Siber dari Joseph Nye (2017) digunakan untuk menganalisis strategi pencegahan dan pertahanan Indonesia terhadap serangan siber China. Libicki (2009) memperkuat konsep ini bahwa *deterrence* siber memiliki karakteristik unik yang membedakannya dari pencegahan nuklir tradisional: atribusi yang sulit, asimetri dampak, dan ketidakpastian tentang kapabilitas lawan menjadikannya lebih kompleks dan kurang dapat diprediksi. Teori ini membantu dalam memahami bagaimana negara dapat mencegah serangan siber melalui kombinasi kapabilitas ofensif, defensif, dan diplomasi. Kerangka Keamanan Siber dari Ronald Deibert dan Rafal Rohozinski (2010) digunakan untuk menganalisis berbagai dimensi ancaman siber, termasuk aspek teknis, sosial, dan politik. Hansen dan Nissenbaum (2009) menambahkan bahwa sekuritisasi domain siber telah menciptakan paradigma baru dalam studi keamanan, di mana ancaman tidak lagi terbatas pada aktor negara dan dampaknya dapat melampaui batas-batas tradisional keamanan nasional. Teori ini membantu dalam memahami kompleksitas lingkungan siber dan berbagai faktor yang mempengaruhi keamanan siber nasional.

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan studi kasus dan studi literatur. Metode ini dipilih untuk memberikan pemahaman mendalam tentang ancaman perang siber China terhadap Indonesia, dengan fokus pada analisis komprehensif terhadap strategi, dampak, dan respons kebijakan.

1. Pendekatan Kualitatif. Pendekatan kualitatif digunakan untuk mengeksplorasi dan memahami kompleksitas fenomena perang siber antara China dan Indonesia. Metode ini memungkinkan peneliti untuk menggali nuansa dan konteks yang mungkin tidak terungkap melalui pendekatan kuantitatif (Creswell & Poth, 2018). Denzin dan Lincoln (2018) menegaskan penelitian kualitatif melibatkan pendekatan naturalistik dan interpretatif terhadap dunia. Ini berarti bahwa para peneliti kualitatif mempelajari hal-hal dalam setting alamiah mereka, berusaha untuk memahami atau menginterpretasikan fenomena dalam hal makna yang dibawa orang kepada mereka.
2. Studi Kasus. Studi kasus dipilih untuk memberikan analisis mendalam tentang situasi spesifik perang siber China terhadap Indonesia. Pendekatan ini memungkinkan peneliti untuk mengeksplorasi berbagai aspek kasus, termasuk konteks historis, geopolitik, dan teknologi (Yin, 2018). Stake (2005), sebagaimana dikutip dalam Denzin dan Lincoln (2018), menyatakan bahwa studi kasus bukanlah pilihan metodologis, tetapi pilihan tentang apa yang akan dipelajari. Kita memilih untuk mempelajari kasus tersebut.
3. Studi Literatur. Studi literatur dilakukan untuk mengumpulkan dan menganalisis data dari berbagai sumber sekunder, termasuk jurnal akademik, laporan pemerintah, artikel berita, dan publikasi think tank. Metode ini membantu dalam membangun pemahaman komprehensif tentang topik dan mengidentifikasi kesenjangan dalam penelitian yang ada (Snyder, 2019). Cooper (2018) menjelaskan bahwa tinjauan literatur yang sistematis adalah metode ilmiah untuk merangkum, mengevaluasi secara kritis, dan mensintesis temuan dari beberapa penelitian.
4. Pengumpulan Data. Miles, Huberman, dan Saldana (2014) menekankan pengumpulan data kualitatif yang efektif membutuhkan triangulasi dari berbagai sumber untuk memastikan kedalaman dan kredibilitas temuan. Patton (2015)

menjelaskan kekuatan pengumpulan data kualitatif terletak pada kemampuannya untuk memberikan deskripsi yang kaya dan penjelasan tentang proses yang terjadi dalam konteks lokal. Data dikumpulkan melalui:

a. Analisis dokumen: kebijakan pemerintah, laporan keamanan siber, dokumen strategis.
b. Studi literatur akademik: jurnal, buku, dan artikel ilmiah terkait perang siber dan hubungan China-Indonesia.
c. Laporan media: berita dan analisis terkait insiden siber antara China dan Indonesia.

5. Analisis Data. Braun dan Clarke (2006) menjelaskan tentang analisis tematik adalah metode untuk mengidentifikasi, menganalisis, dan melaporkan pola (tema) dalam data. Ini minimal mengorganisir dan mendeskripsikan dataset Anda secara detail. Silverman (2016) menegaskan bahwa analisis data kualitatif yang baik bergantung pada pemahaman mendalam tentang konteks dan kemampuan untuk mengidentifikasi pola yang bermakna dalam data:
   a. Coding tematik: mengidentifikasi tema-tema utama dalam data yang dikumpulkan.
   b. Analisis konten: memeriksa isi dokumen dan literatur untuk mengidentifikasi pola dan tren.
   c. Triangulasi: membandingkan dan mengkonfirmasi temuan dari berbagai sumber untuk meningkatkan validitas.

Melalui metode penelitian ini, diharapkan dapat diperoleh pemahaman yang mendalam dan komprehensif tentang ancaman perang siber China terhadap Indonesia, serta menghasilkan rekomendasi yang relevan dan aplikatif untuk meningkatkan ketahanan siber Indonesia.

HASIL PENELITIAN DAN DISKUSI

Hasil penelitian ini disajikan dan dibahas dalam beberapa bagian utama, yang mencakup karakteristik dan strategi perang siber China terhadap Indonesia, dampaknya terhadap keamanan nasional Indonesia, respons kebijakan Indonesia, dan analisis kesenjangan serta tantangan yang dihadapi.

Karakteristik dan Strategi Perang Siber China terhadap Indonesia

Pola Serangan

Hasil analisis menunjukkan bahwa serangan siber China terhadap Indonesia memiliki pola yang konsisten dan semakin canggih. Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN), terjadi peningkatan signifikan dalam jumlah dan kompleksitas serangan siber yang berasal dari China sejak tahun 2018 (BSSN, 2023). Karakteristik utama serangan siber China meliputi:

a. *Advanced Persistent Threats* (APT): Kelompok seperti *Mustang Panda* dan *Naikon APT* melakukan operasi jangka panjang dan terencana.
b. *Spear-phishing*: Penggunaan email yang ditargetkan untuk menipu pejabat pemerintah dan eksekutif perusahaan.
c. *Malware canggih*: Penggunaan malware yang sulit dideteksi dan memiliki kemampuan untuk mengumpulkan data sensitif.

Target Utama

Analisis menunjukkan bahwa target utama serangan siber China di Indonesia meliputi:

a. Lembaga pemerintah: Kementerian Pertahanan, Kementerian Luar Negeri, dan badan intelijen.
b. Infrastruktur kritis: Sektor energi, telekomunikasi, dan transportasi.
c. Perusahaan strategis: BUMN dan perusahaan swasta di sektor teknologi dan sumber daya alam.

Motivasi dan Tujuan

Berdasarkan analisis dokumen strategis China dan pola serangan, motivasi utama perang siber China terhadap Indonesia meliputi:

a. Espionase ekonomi: Pencurian kekayaan intelektual dan informasi bisnis strategis.
b. Intelijen militer: Pengumpulan data tentang kapabilitas pertahanan Indonesia.
c. Pengaruh politik: Upaya untuk mempengaruhi kebijakan Indonesia terkait isu-isu sensitif seperti Laut China Selatan.

Temuan ini sejalan dengan Teori Peperangan Asimetris Mack (1975), di mana China sebagai negara dengan kapabilitas siber yang lebih kuat memanfaatkan keunggulannya untuk mencapai tujuan strategis tanpa konfrontasi militer langsung. Strategi ini memungkinkan China untuk memperoleh keuntungan geopolitik dan ekonomi dengan risiko eskalasi yang relatif rendah.

Dampak terhadap Keamanan Nasional Indonesia

Kerentanan Infrastruktur Kritis

Hasil penelitian menunjukkan bahwa serangan siber China telah mengekspos kerentanan signifikan dalam infrastruktur kritis Indonesia. Insiden seperti peretasan sistem kontrol pembangkit listrik di Jawa Barat pada tahun 2022 (BSSN, 2023) menunjukkan potensi dampak serius terhadap keamanan energi nasional.

Kebocoran Data Sensitif

Analisis menunjukkan terjadinya beberapa kasus kebocoran data sensitif, termasuk:

a. Dokumen kebijakan pertahanan dari Kementerian Pertahanan (2021).
b. Data pribadi 100 juta warga Indonesia dari sistem e-KTP (2020).
c. Informasi keuangan dari beberapa bank BUMN (2019-2022).

Gangguan Ekonomi

Serangan siber telah menyebabkan gangguan ekonomi, termasuk:

a. Kerugian finansial langsung akibat penipuan siber dan pemerasan.
b. Penurunan kepercayaan investor terhadap keamanan data di Indonesia.
c. Biaya tambahan untuk pemulihan sistem dan peningkatan keamanan.

Dampak ini menegaskan relevansi Teori Pertahanan Nasional Buzan (1991), yang menekankan interkoneksi antara berbagai dimensi keamanan. Serangan siber tidak hanya berdampak pada aspek teknologi, tetapi juga mempengaruhi

keamanan ekonomi, politik, dan sosial Indonesia. Hal ini menunjukkan perlunya pendekatan komprehensif dalam strategi pertahanan siber nasional.

Respons Kebijakan Indonesia

Keamanan siber di Indonesia mulai berkembang di penghujung dekade 1990-an, sejalan dengan meluasnya penggunaan internet di masyarakat. Meski demikian, dibandingkan negara-negara tetangga seperti Malaysia dan Singapura, Indonesia tertinggal dalam menetapkan regulasi keamanan siber. Sebagai contoh, Malaysia sudah memiliki *Computer Crime Act* dan *Multimedia Act* pada tahun 1997 (Leonardus et al., 2016). Memasuki abad ke-21, ancaman siber di Indonesia meningkat tajam. Pada tahun 2002, negara ini menduduki peringkat kedua tertinggi dalam kasus penipuan online. Insiden- insiden serius, seperti peretasan website KPU saat Pemilu 2004, mengindikasikan kurangnya perhatian pemerintah terhadap masalah keamanan siber. Saat ini, Indonesia menghadapi urgensi untuk menangani keamanan siber karena tingkat kejahatan dunia maya telah mencapai level yang mengkhawatirkan. Data CIA menunjukkan bahwa kerugian akibat kejahatan siber di Indonesia mencapai 1,20% dari total kerugian global (Handrini, 2014). Mengingat kompleksitasnya, penanganan keamanan siber membutuhkan pendekatan kebijakan yang menyeluruh, berbeda dari penanganan kejahatan konvensional. Perkembangan hukum keamanan siber di Indonesia dapat ditelusuri melalui penerapan dua undang-undang penting: UU Telekomunikasi No.36/1999 dan UU Informasi dan Transaksi Elektronik (ITE) No.11/2008. Kedua regulasi ini merupakan upaya pemerintah Indonesia untuk mengatur keamanan komunikasi teknologi secara umum di negara ini. UU Telekomunikasi, yang disahkan oleh Presiden B.J. Habibie dan Menteri Sekretaris Negara Muladi, merupakan langkah awal dalam merumuskan kebijakan khusus terkait aktivitas telekomunikasi di Indonesia. Undang-undang ini mencakup berbagai bentuk komunikasi berbasis teknologi yang ada saat itu, termasuk televisi, radio, dan telepon.

Sebagai respons terhadap meningkatnya ancaman siber, berbagai pemangku kepentingan utama di Indonesia, termasuk KEJAGUNG, POLRI, APJII, AWARI, dan MASTI, menginisiasi pembentukan Tim Respons Insiden Keamanan Siber Indonesia pada Infrastruktur Internet (ID-SIRTII). Lembaga ini bertugas memantau, mendeteksi dini, memberi peringatan terhadap ancaman jaringan, serta berkolaborasi dengan pihak dalam dan luar negeri. Kerangka hukum keamanan siber di Indonesia secara umum didasarkan pada UU ITE No. 11/2008, PP No. 82/2012, serta regulasi dari kementerian terkait. Meskipun demikian, Indonesia masih menghadapi beberapa tantangan nasional dalam bidang keamanan siber, antara lain:

1. Kurangnya pemahaman di kalangan pemangku kepentingan tentang keamanan dunia maya
2. Kebutuhan akan landasan hukum yang memadai untuk menangani serangan siber
3. Pengelolaan kelembagaan yang belum komprehensif
4. Kelemahan industri dalam pengembangan perangkat keras terkait teknologi informasi Tantangan-tantangan ini menunjukkan perlunya upaya lebih lanjut dalam meningkatkan keamanan siber di Indonesia.

Badan Siber dan Sandi Negara (BSSN) dibentuk melalui Peraturan Presiden No.53/2017 sebagai lembaga pemerintah non-kementerian yang bertanggung jawab langsung kepada presiden. BSSN, yang menggantikan Lembaga Sandi Negara (LSN),

memiliki tugas utama mengelola keamanan sandi di Indonesia. Lembaga ini juga berperan dalam implementasi kebijakan teknis terkait identifikasi, deteksi, perlindungan, penanggulangan, dan pemantauan keamanan siber nasional, melanjutkan fungsi yang sebelumnya dijalankan oleh ID-SIRTII (Maulia, 2017: 141). Selain BSSN, beberapa lembaga pemerintah lainnya juga memiliki peran dalam keamanan siber, termasuk Polri, Kementerian Pertahanan (Kemhan), Badan Intelijen Negara (BIN), dan Tentara Nasional Indonesia. Masing-masing lembaga ini memiliki kebijakan dan tanggung jawab spesifik dalam bidang keamanan siber. Meskipun demikian, pendekatan keamanan di Indonesia masih cenderung berorientasi pada negara daripada individu. Hal ini mengakibatkan kurangnya strategi keamanan siber yang komprehensif. Walaupun perlindungan hak individu di dunia maya dianggap krusial, keterbatasan regulasi, terutama belum adanya Undang-Undang khusus tentang keamanan siber, menjadi hambatan dalam menegakkan keamanan tersebut secara efektif. Situasi ini menunjukkan perlunya pengembangan lebih lanjut dalam kebijakan dan regulasi keamanan siber di Indonesia, dengan fokus yang lebih seimbang antara kepentingan negara dan perlindungan hak-hak individu di ranah digital.

Pengembangan Kerangka Hukum

Indonesia telah mengambil langkah-langkah untuk memperkuat kerangka hukum terkait keamanan siber, termasuk:

a. Pengesahan UU Perlindungan Data Pribadi pada tahun 2022.
b. Revisi UU ITE untuk mencakup aspek keamanan siber yang lebih komprehensif.

Penguatan Kapabilitas Pertahanan Siber

Upaya peningkatan kapabilitas pertahanan siber meliputi:

a. Pembentukan Badan Siber dan Sandi Negara (BSSN) sebagai lembaga utama keamanan siber nasional.
b. Investasi dalam teknologi deteksi dan respons insiden siber.
c. Pelatihan dan pengembangan SDM keamanan siber.

Kerjasama Internasional

Indonesia telah meningkatkan kerjasama internasional dalam bidang keamanan siber, termasuk:

a. Partisipasi aktif dalam *ASEAN Cybersecurity Cooperation Strategy*.
b. Kerjasama bilateral dengan negara-negara maju seperti AS, Jepang, dan Australia dalam pengembangan kapabilitas siber.

Respons kebijakan Indonesia menunjukkan upaya untuk menerapkan konsep *Deterrence* Siber dari Nye (2017). Melalui kombinasi pengembangan kapabilitas defensif, kerangka hukum yang kuat, dan kerjasama internasional, Indonesia berusaha meningkatkan biaya dan risiko bagi penyerang potensial, termasuk China. Namun, efektivitas strategi ini masih terbatas karena adanya kesenjangan kapabilitas yang signifikan.

Kesenjangan dan Tantangan

Kesenjangan Teknologi

Indonesia masih menghadapi kesenjangan teknologi yang signifikan dibandingkan dengan China dalam hal:

a. Infrastruktur keamanan siber canggih.
b. Kemampuan analisis big data dan kecerdasan buatan untuk deteksi ancaman.
c. Teknologi enkripsi dan perlindungan data tingkat lanjut.

Kekurangan SDM

Terdapat kekurangan serius dalam jumlah dan kualitas tenaga ahli keamanan siber di Indonsia, yang meliputi:

a. Kurangnya profesional keamanan siber bersertifikasi.
b. Kesenjangan antara kurikulum pendidikan dan kebutuhan industri.
c. *Brain drain* ahli keamanan siber ke negara lain atau perusahaan multinasional.

Koordinasi Antar Lembaga

Tantangan dalam koordinasi antar lembaga pemerintah dan sektor swasta, termasuk:

a. Tumpang tindih wewenang antara BSSN, Kemenkominfo, dan lembaga penegak hukum.
b. Kurangnya mekanisme berbagi informasi yang efektif antara pemerintah dan sektor swasta.
c. Perbedaan prioritas dan pendekatan dalam menangani ancaman siber.

Kesenjangan dan tantangan ini mencerminkan kompleksitas yang dihadapi Indonesia dalam membangun ketahanan siber, sesuai dengan Kerangka Keamanan Siber Deibert dan Rohozinski (2010). Faktor-faktor teknis, sosial, dan politik saling berinteraksi, menciptakan tantangan multidimensi yang memerlukan pendekatan holistik dan jangka panjang.

KESIMPULAN

Penelitian ini mengungkapkan bahwa ancaman siber China terhadap Indonesia memiliki karakteristik yang kompleks dan canggih. Serangan-serangan yang dilakukan mencakup *Advanced Persistent Threats* (APT), spear-phishing, dan penggunaan malware canggih. Target utama meliputi lembaga pemerintah, infrastruktur kritis, dan perusahaan strategis di Indonesia. Motivasi di balik serangan ini meliputi espionase ekonomi, intelijen militer, dan upaya mempengaruhi kebijakan Indonesia. Serangan siber China telah mengekspos kerentanan signifikan dalam infrastruktur kritis Indonesia, menyebabkan kebocoran data sensitif, dan menimbulkan gangguan ekonomi. Dampak ini tidak hanya terbatas pada aspek teknologi, tetapi juga mempengaruhi dimensi keamanan ekonomi, politik, dan sosial Indonesia. Indonesia telah mengambil langkah-langkah untuk meningkatkan pertahanan sibernya, termasuk pengembangan kerangka hukum, penguatan kapabilitas pertahanan siber, dan peningkatan kerjasama internasional. Namun, efektivitas respons ini masih terbatas karena adanya kesenjangan kapabilitas yang signifikan. Indonesia masih menghadapi kesenjangan teknologi yang signifikan, kekurangan SDM di bidang keamanan siber, dan tantangan dalam koordinasi antar lembaga. Faktor- faktor ini membatasi kemampuan Indonesia untuk menghadapi ancaman siber China secara efektif. Temuan penelitian menunjukkan bahwa menghadapi ancaman siber China memerlukan pendekatan komprehensif yang mencakup aspek teknologi, kebijakan, sumber daya manusia, dan kerjasama internasional. Strategi pertahanan siber Indonesia perlu dikembangkan dengan mempertimbangkan kompleksitas dan dinamika ancaman yang berubah cepat.

Saran

1. Peningkatan Investasi dalam Teknologi dan Infrastruktur: Alokasikan anggaran yang lebih besar untuk pengembangan dan pembaruan infrastruktur keamanan siber nasional. Investasikan dalam teknologi deteksi dan respons ancaman canggih, termasuk sistem berbasis kecerdasan buatan dan machine learning. Kembangkan pusat operasi keamanan siber (Security Operations Center) nasional yang terintegrasi untuk monitoring dan respons real-time.
2. Pengembangan Sumber Daya Manusia: Tingkatkan kualitas dan kuantitas program pendidikan dan pelatihan keamanan siber di tingkat perguruan tinggi dan vokasi. Implementasikan program sertifikasi nasional untuk profesional keamanan siber dengan standar internasional. Luncurkan inisiatif nasional untuk menarik dan mempertahankan bakat di bidang keamanan siber, termasuk insentif finansial dan pengembangan karir.
3. Penguatan Kerangka Hukum dan Regulasi: Revisi dan perkuat UU ITE dan UU Perlindungan Data Pribadi untuk mengakomodasi perkembangan ancaman siber terkini. Kembangkan regulasi spesifik untuk perlindungan infrastruktur kritis dari ancaman siber. Harmonisasikan kerangka hukum keamanan siber Indonesia dengan standar internasional untuk memfasilitasi kerjasama lintas batas.
4. Peningkatan Koordinasi dan Kerjasama: Bentuk gugus tugas keamanan siber nasional yang melibatkan berbagai lembaga pemerintah, sektor swasta, dan akademisi. Implementasikan mekanisme berbagi informasi ancaman siber yang efektif antara pemerintah dan sektor swasta. Tingkatkan kerjasama dengan CERT (*Computer Emergency Response Team*) internasional untuk pertukaran informasi dan best practices.
5. Penguatan Diplomasi Siber: Tingkatkan peran aktif Indonesia dalam forum keamanan siber internasional, terutama di tingkat ASEAN dan Asia Pasifik. Inisiasi dialog bilateral keamanan siber dengan China untuk membangun pemahaman bersama dan mengurangi risiko eskalasi. Kembangkan aliansi keamanan siber regional untuk menghadapi ancaman bersama.
6. Peningkatan Kesadaran dan Literasi Siber: Luncurkan kampanye nasional untuk meningkatkan kesadaran keamanan siber di kalangan masyarakat umum, bisnis, dan lembaga pemerintah. Integrasikan pendidikan keamanan siber ke dalam kurikulum sekolah dari tingkat dasar hingga menengah. Selenggarakan latihan dan simulasi serangan siber secara regular untuk meningkatkan kesiapsiagaan nasional.
7. Pengembangan Industri Keamanan Siber Domestik: Berikan insentif untuk pengembangan startup dan perusahaan keamanan siber lokal. Dorong kerjasama antara industri, akademisi, dan pemerintah dalam penelitian dan pengembangan solusi keamanan siber. Fasilitasi transfer teknologi melalui kerjasama dengan perusahaan keamanan siber internasional terkemuka.
8. Implementasi Strategi Deterrence Siber: Kembangkan dan komunikasikan doktrin pertahanan siber nasional yang jelas. Tingkatkan kapabilitas ofensif siber sebagai bagian dari strategi deterrence, namun dengan pengawasan dan kontrol yang ketat. Bangun mekanisme atribusi serangan siber yang kredibel untuk mendukung respons diplomatik dan hukum.
9. Perlindungan Infrastruktur Kritis: Implementasikan standar keamanan siber yang ketat untuk semua infrastruktur kritis nasional. Lakukan audit dan penilaian risiko siber secara regular terhadap infrastruktur kritis. Kembangkan rencana

kontingensi dan pemulihan bencana siber untuk setiap sektor infrastruktur kritis.

10. Penelitian dan Pengembangan: Tingkatkan pendanaan untuk penelitian keamanan siber di universitas dan lembaga penelitian nasional. Fokuskan pada pengembangan teknologi keamanan siber indigenous yang sesuai dengan kebutuhan dan konteks Indonesia. Dorong kolaborasi penelitian internasional dalam bidang keamanan siber, terutama dengan negara-negara yang memiliki kapabilitas maju.

Implementasi rekomendasi-rekomendasi ini memerlukan komitmen jangka panjang, koordinasi yang kuat antar pemangku kepentingan, dan alokasi sumber daya yang signifikan. Namun, mengingat sifat kritis dari ancaman siber yang dihadapi Indonesia, investasi dalam meningkatkan ketahanan siber nasional adalah langkah yang tidak dapat ditunda lagi. Dengan pendekatan komprehensif dan strategis, Indonesia dapat meningkatkan posisinya dalam menghadapi ancaman siber dari China dan aktor lainnya, serta melindungi kepentingan nasionalnya di era digital.

DAFTAR PUSTAKA

Arreguin-Toft, I. (2001). How the weak win wars: A theory of asymmetric conflict. International Security, 26(1), 93-128.

Badan Siber dan Sandi Negara. (2023). *Laporan tahunan keamanan siber nasional 2022*. BSSN.

Baldwin, D. A. (1997). The concept of security. Review of International Studies, 23(1), 5-26.

Ball, D. (2011). China's Cyber Warfare Capabilities. *Security Challenges*, *7*(2), 81–103. http://www.jstor.org/stable/26461991

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101.

Buzan, B. (1991). People, states and fear: An agenda for international security studies in the post-cold war era (2nd ed.). Harvester Wheatsheaf.

Buzan, B. (2009). People, states & fear: An agenda for international security studies in the post-cold war era. ECPR Press.

Calfee, R. C., & Valencia, R. R. (1991). *APA guide to preparing manuscripts for journal publication.* Washington, DC: American Psychological Association.

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. International Affairs, 92(1), 43-62. https://doi.org/10.1111/1468-2346.12504

Cooper, H. (2018). Research synthesis and meta-analysis: A step-by-step approach (5th ed.). SAGE Publications.

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.

Creswell, J. W., & Poth, C. N. (2018). Qualitative Inquiry and Research Design: Choosing Among Five Approaches. SAGE Publications.

Deibert, R. J., & Rohozinski, R. (2010). Risking security: Policies and paradoxes of cyberspace security. International Political Sociology, 4(1), 15-32. https://doi.org/10.1111/j.1749-5687.2009.00088.x.

Deibert, R., & Rohozinski, R. (2010). Risking security: Policies and paradoxes of cyberspace security. International Political Sociology, 4(1), 15-32.

Denzin, N. K. (2017). Qualitative Inquiry and Research Design: Choosing Among Five Approaches. SAGE Publications.

Denzin, N. K., & Lincoln, Y. S. (Eds.). (2018). The SAGE handbook of qualitative research (5th ed.). SAGE Publications.

Fink, A. (2020). Conducting Research Literature Reviews: From the Internet to Paper (5th ed.). SAGE Publications.

Gady, F. S., & Austin, G. (2010). Russia, the United States, and cyber diplomacy: Opening the doors. EastWest Institute.

Handrini Ardiyanti: Cyber security dan Tantangan Pengembangannya di Indonesia, Politica Vol. 5 No. 1 Juni 2014.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. International Studies Quarterly, 53(4), 1155-1175.

Hart, C. (2018). Doing a Literature Review: Releasing the Research Imagination. SAGE Publications.

Hjortdal, M. (2011). China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security*, *4*(2), 1–24. http://www.jstor.org/stable/26463924.

Islami, Maulia J. (2017). Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau dari Penilaian Global Cybersecurity Index. Jurnal Masyarakat Telematika dan Informasi, Vol. 8, No. 2 (Oktober-Desember 2017). Jakarta Pusat, Indonesia: Kemenkominfo

Kementerian Komunikasi dan Informatika. (2022). Strategi keamanan siber nasional Indonesia 2020-2024. Kominfo.

Kolton, Michael. "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence." *The Cyber Defense Review* 2, no. 1 (2017): 119–54. http://www.jstor.org/stable/26267405.

Libicki, M. C. (2009). Cyberdeterrence and cyberwar. RAND Corporation. Libicki, M. C. (2016). Cyberspace in Peace and War. Naval Institute Press.

Lindsay, J. R., Cheung, T. M., & Reveron, D. S. (Eds.). (2015). China and cybersecurity: Espionage, strategy, and politics in the digital domain. Oxford University Press.

Mack, A. (1975). Why big nations lose small wars: The politics of asymmetric conflict. World Politics, 27(2), 175-200. https://doi.org/10.2307/2009880

Marshall, C., & Rossman, G. B. (2016). Designing Qualitative Research (6th ed.). SAGE Publications.

Merriam, S. B. (2019). Qualitative Research and Case Study Applications in Education. Jossey-Bass Publishers.

Miles, M. B., Huberman, A. M., & Saldana, J. (2014). Qualitative data analysis: A methods sourcebook (3rd ed.). SAGE Publications.

Nugraha, Leonardus K. dan Putri, Dinita A. (2016). Mapping the Cyber Policy Landscape: Indonesia. London, England: Global Partners Digital

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. International Security, 41(3), 44-71. https://doi.org/10.1162/ISEC_a_00266

Patton, M. Q. (2015). Qualitative research & evaluation methods (4th ed.). SAGE Publications.

Petticrew, M., & Roberts, H. (2006). Systematic reviews in the social sciences: A practical guide. Blackwell Publishing.

Putra, I. E., & Firdaus, A. (2021). Analisis ancaman siber terhadap keamanan nasional Indonesia. Jurnal Keamanan Nasional, 7(1), 25-42. https://doi.org/10.31599/jkn.v7i1.519

Putra, I. E., Darwis, & Janitra, P. A. (2020). Tantangan Keamanan Siber Indonesia di Era Digitalisasi: Analisis SWOT Keamanan Siber Indonesia. Jurnal Teknologi Informasi

dan Ilmu Komputer, 7(6), 1241-1250.
Rid, T. (2012). Cyber war will not take place. Journal of Strategic Studies, 35(1), 5-32. https://doi.org/10.1080/01402390.2011.608939
Rid, T. (2017). Cyber War Will Not Take Place. Oxford University Press.
Rizal, M., & Yani, Y. M. (2016). Cybersecurity Policy and Its Implementation in Indonesia. Journal of ASEAN Studies, 4(1), 61-78.
Sari, R. F. (2019). Cybersecurity: Challenges and opportunities for Indonesia. Journal of Physics: Conference Series, 1361(1), 012017.
Segal, A. (2016). The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age. PublicAffairs.
Setiadi, F., Sucahyo, Y. G., & Hasibuan, Z. A. (2012). An overview of the development Indonesia national cyber security. International Journal of Information Technology & Computer Science, 6, 106-114.
Silverman, D. (2016). Qualitative research (4th ed.). SAGE Publications.
Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333-339.
Stake, R. E. (2005). Qualitative case studies. In N. K. Denzin & Y. S. Lincoln (Eds.), The SAGE handbook of qualitative research (3rd ed., pp. 443-466). SAGE Publications.
Stake, R. E. (2020). The Art of Case Study Research. SAGE Publications.
Valeriano, B., & Maness, R. C. (2015). Cyber war versus cyber realities: Cyber conflict in the international system. Oxford University Press.
Walt, S. M. (2018). The Origins of Alliances. Cornell University Press. Waltz, K. N. (2019). Theory of International Politics. Waveland Press.
Wang, D., & Mark, G. (2015). Internet censorship in China: Examining user awareness and attitudes. ACM Transactions on Computer-Human Interaction, 22(6), 1-22. https://doi.org/10.1145/2818997
Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications. https://www.unav.edu/web/global-affairs/chinese-cyber-warfare-in-the-indo-pacific