Menghadapi *Cyberwarfare*: Strategi Perdana Menteri Anthony Albanese Untuk Melindungi Infrastruktur Digital Australia

Muhamad Zahrofi Adifkia
Prodi Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Wahid Hasyim
e-mail: muhamadzadifkia@gmail.com

Anna Yulia Hartati
Prodi Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Wahid Hasyim
e-mail: muhamadzadifkia@gmail.com

Abstrak

Cyberwarfare merupakan salah satu tantangan keamanan yang paling signifikan di era digital saat ini. Negara-negara seperti Australia yang sangat bergantung pada teknologi digital untuk infrastruktur kritikalnya, menghadapi risiko besar terhadap serangan cyber. Artikel ini membahas ancaman cyber warfare terhadap Australia, mengidentifikasi infrastruktur kritikal yang rentan, dan strategi-strategi yang diambil Anthony untuk menguatkan pertahanan digital. Tulisan ini menggunakan metode kualitatif yang mengandalkan analisis dokumen dan studi literatur, membahas fenomena tersebut dengan menggunakan teori Strategi Keamanan Nasional sebagai kerangka berpikir utama.
Kata kunci: *Cyber Warfare*, Infrastruktur Digital, Keamanan Siber, Australia, Perlindungan Digital.

Abstract

Cyberwarfare is one of the most significant security challenges in today's digital age. Countries like Australia that rely heavily on digital technology for their critical infrastructure, face a huge risk of cyberattacks. This article discusses the threat of cyber warfare against Australia, identifying vulnerable critical infrastructure, and the strategies Anthony has taken to strengthen digital defence. This paper uses qualitative methods that rely on document analysis and literature studies, dealing with phenomena using the National Security Strategy theory as a primary thinking framework.
Keywords*: Cyber Warfare, Digital Infrastructure, Cyber Security, Australia, Digital Protection.*

Pendahuluan

Di era teknologi modern, menjaga keamanan siber adalah keharusan. Dengan meningkatnya serangan siber di seluruh dunia, perlu ada strategi keamanan siber yang komprehensif untuk melindungi infrastruktur digital suatu negara. Australia, sebagai negara yang terus berkembang dalam teknologi dan digitalisasi, menghadapi tantangan yang semakin besar dalam mempertahankan keamanan sibernya. Oleh karena itu, pengembangan *cyber security strategy*

oleh pemerintah Australia, khususnya strategi yang dikembangkan di bawah kepemimpinan Perdana Menteri Anthony Albanese, menjadi sangat penting dalam upaya menjaga keamanan nasional serta melindungi kepentingan publik dan sektor swasta dari ancaman siber.

Menurut *Australian Cyber Security Centre* (ACSC), terdapat lebih dari 94,000 laporan kejahatan siber yang diterima pada tahun 2022-2023, bukan lebih dari 10 juta serangan siber yang teridentifikasi pada tahun 2021. Laporan ini menunjukkan bahwa ASD menerima lebih dari 33,000 panggilan ke *Australian Cyber Security Hotline*, dan lebih dari 10% dari insiden siber yang direspons terkait dengan serangan menggunakan ransomware.

Dari laporan tersebut, kemampuan siber negara mengancam Australia. Selain itu, fakta bahwa kejahatan dunia maya terus mengubah taktik destruktif mereka untuk mendapatkan keuntungan maksimal dari kejahatan mereka, menunjukkan bahwa kejahatan dunia maya masih menjadi ancaman besar bagi masyarakat Australia. Jutaan warga Australia terkena dampak pelanggaran data pada tahun keuangan terakhir, dan penipuan dan penipuan terus- menerus membahayakan mereka. Aktor ancaman dapat dengan cepat menggunakan kerentanan kritis sistem dan jaringan Australia, terkadang melakukan serangan dalam hitungan jam. Laporan Ancaman Siber Tahunan tersebut mendorong setiap orang Australia untuk berpartisipasi dalam melindungi masa depan keamanan siber negaranya.

Artikel ini akan membahas berbagai aspek penting dari *Australian cyber security strategy*, termasuk paham tentang *cyber warfare*, ancaman terhadap infrastruktur digital Australia, dan langkah-langkah yang diambil oleh Perdana Menteri Anthony Albanese untuk menghadapi tantangan tersebut. Lebih lanjut, akan dibahas mengenai strategi keamanan digital Australia 2023-2030, peran kerjasama internasional dalam memperkuat sistem keamanan siber, pentingnya meningkatkan kesadaran publik tentang risiko keamanan siber, investasi pada teknologi keamanan, serta evaluasi dan monitoring sebagai bagian dari sistem pengawasan. Pendekatan ini tidak hanya membantu dalam memperkuat keamanan digital di tingkat nasional melalui *national cyber security strategy*, tetapi juga mendukung kerjasama global dalam mencegah dan menanggapi ancaman siber.

Metode Penelitian

Penulis menggunakan metode kualitatif dalam artikel jurnal ini. Studi kepustakaan atau studi literatur yang mefokuskan pada pendekatan adalah sumber data utama. Penelitian jenis ini juga dapat disebut sebagai upaya untuk menafsirkan fenomena dengan meminta interpretasi orang lain untuk melengkapi pemahaman kita. Jenis penelitian ini eksploratif, fleksibel, digerakkan oleh data, dan peka terhadap konteks. Dua metode pengumpulan data digunakan dalam penelitian ini yaitu studi literatur dan analisis data. Studi literatur adalah upaya peneliti untuk meninjau berbagai jenis literatur yang berkaitan dengan topik tersebut, seperti buku, artikel jurnal, ilmu sosial, dan berita, dan kemudian melakukan analisis menyeluruh dari bahan-bahan tersebut dengan menggunakan Teori Strategi Keamanan Nasional sebagai kerangka berpikir utama.

Hasil Dan Pembahasan

Mengerti *Cyberwarfare*

Cyberwarfare adalah serangan *cyber* yang dilakukan oleh satu negara atau organisasi internasional untuk menyerang dan berusaha merusak komputer atau jaringan informasi negara lain melalui virus komputer atau serangan penolakan layanan. Istilah ini berbeda dengan *cyber war*, di mana *cyberwarfare* mencakup teknik, taktik, dan prosedur yang mungkin terlibat dalam perang dunia maya, sementara *cyber war* menggambarkan periode serangan siber yang berlarut-larut, digabungkan dengan tindakan militer konvensional.

Cyber warfare merupakan perkembangan dari *cyberattack* dan *cybercrime*. *Cyb erwarfare* dapat diartikan sebagai perang di dalam *cyberspace*, namun di dalam *cyber warfare* terdapat penyerangan yang berbeda dengan penyerangan dalam perang konvensional atau perang fisik lainnya. Dalam *cyberwarfare*, media utama yang digunakan adalah komputer dan internet. Objek yang diserang dalam *cyberwarfare* bukan merupakan wilayah fisik, teritorial, atau geografis, tetapi dalam *cyberspace* yang dikuasai oleh suatu negara.
The United Nations Terminology Database (UNTERM) mendefinisikan *cyberwarfare* sebagai tindakan militer yang memanfaatkan teknologi untuk merusak atau mencuri informasi milik target untuk keuntungan perusahaan dan militer. Sementara *The United Nations Interregional Crime and Justice Reseearch Institute* (UNICRI) mendefinisikan *cyberwarfare* sebagai

> "*any action by a nation-state to penetrate another nation's computer networks for the purpose of causing some sort of damage*",

definisi ini serupa dengan definisi Richard Clarke, yang mendefinisikan *cyberwarfare* sebagai tindakan aktor negara untuk memasuki jaringan komputer negara lain dengan tentara, menyebabkan kerusakan.

Jenis-jenis *Cyberwafare.*

Serangan siber dapat bervariasi, mulai dari *phishing*, di mana penyerang memancing korban dengan email atau pesan yang tampak sah untuk mencuri informasi sensitif. Virus komputer adalah jenis lain dari serangan siber, yang dapat merusak atau mengganggu operasi sistem dengan menyamar sebagai file yang sah. *Trojan*, sejenis malware, dirancang untuk memata-matai atau merusak sistem tanpa diketahui oleh pengguna. *Worm* adalah program yang dapat menggandakan diri dan menyebar melalui jaringan, menyebabkan kerusakan luas. Serangan *Denial of Service* (DoS) bertujuan untuk melumpuhkan jaringan atau layanan dengan membanjiri target dengan lalu lintas yang berlebihan. *Advanced Persistent Threats* (APT) adalah serangan yang dilakukan secara terus menerus dan bertujuan untuk mencuri data dari target selama periode waktu yang lama. Serangan injeksi SQL dan *Cross- Site Scripting* (XSS) adalah contoh serangan yang memanfaatkan kelemahan dalam kode aplikasi untuk mencuri data atau mengambil alih sesi pengguna. *Ransomware*, serangan yang semakin umum, mengenkripsi data korban dan menuntut tebusan untuk dekripsi. Setiap jenis serangan ini memiliki potensi yang signifikan

untuk merusak infrastruktur kritis dan mengganggu layanan penting, menekankan pentingnya strategi keamanan siber yang efektif.

Ancaman terhadap Infrastruktur Digital Australia

Australian Cyber Security Centre (ACSC) melaporkan bahwa mereka menerima satu laporan kejahatan dunia maya setiap 8 menit selama setahun terakhir, menunjukkan tingginya tingkat ancaman terhadap infrastruktur digital. Dengan satu dari empat insiden serangan siber menargetkan infrastruktur dan layanan penting, terutama selama banyak orang bekerja dari rumah karena pandemi, risiko terhadap keamanan nasional menjadi semakin serius.

Mereka mengklaim bahwa Australia telah menjadi sasaran serangan dari "aktor siber canggih berbasis negara" yang menargetkan semua tingkat pemerintahan, partai politik, dan penyedia layanan penting. Pada Juli 2020, Amerika Serikat dan sekutunya, termasuk Australia, menuduh China melakukan kampanye spionase dunia maya. Serangan ini menyebabkan kerugian ekonomi yang signifikan, dengan taksiran kerugian hingga 29 miliar dollar Australia atau setara Rp 302,5 triliun.

Serangan siber dapat menyerang sektor energi. Infrastruktur energi, termasuk jaringan listrik dan pembangkit listrik, sangat penting untuk kelangsungan hidup masyarakat negara. Jika terjadi gangguan pada infrastruktur energi suatu negara, maka di negara tersebut akan terjadi pemadaman listrik, kerusakan ekonomi besar, dan bahkan bahaya jiwa. Infrastruktur energi dapat dengan mudah dilumpuhkan oleh serangan *cyber*, menjadikannya tujuan yang menarik bagi penjahat siber. Pemerintah Australia sedang memperbarui Undang-Undang Keamanan Infrastruktur Kritikal tahun 2018. Kerangka regulasi yang diperbarui mencakup sebelas industri, termasuk energi, dalam revisi undang-undang ini. Organisasi sektor energi harus menerapkan strategi manajemen risiko semua bahaya dengan fokus pada risiko siber dan informasi, fisik, personil, rantai pasokan, dan risiko bencana alam[6]. Selain sektor energi, serangan siber juga dapat menyerang sektor kesehatan. Infrastruktur kesehatan, termasuk peralatan medis dan layanan informasi, rawan terhadap serangan siber**.** Infrastruktur kesehatan menyimpan data sensitif pasien, seperti rekam medis dan informasi keuangan, yang menjadi target utama penjahat siber. Dizaman sekarang ini, industri kesehatan semakin bergantung pada teknologi, hal itu dapat membuka celah bagi serangan siber. Banyak staf kesehatan juga yang kurang sadar akan risiko keamanan siber, sehingga mudah dimanipulasi oleh penjahat siber.

Salah satu insiden kebocoran data terbesar di Australia terjadi pada perusahaan telekomunikasi Optus, di mana data dari 10 juta pelanggan diretas. Insiden ini menjadi 'seruan peringatan besar' bagi sektor perusahaan dan mendorong pemerintah untuk memperketat aturan privasi dan meningkatkan pertahanan siber. Ancaman umum terhadap keamanan informasi di sektor kesehatan meliputi *ransomware, remote access trojan* (RAT), *phishing*, dan serangan DDoS/botnets. Penyalahgunaan data Optus, yang terjadi pada bulan September 2022 kemarin, dianggap sebagai salah satu pelanggaran data terbesar dalam sejarah Australia. Pelanggaran ini mempengaruhi sekitar 10 juta pelanggan, dengan peretas mendapatkan akses tidak sah ke informasi pribadi mereka, termasuk nama, tanggal lahir, alamat, nomor telepon, informasi paspor, nomor lisensi pengemudi, nomor ID pemerintah, dan catatan medis. *Australian*

Communications and Media Authority (ACMA) mengklaim bahwa Optus gagal melindungi informasi pribadi pelanggan karena kesalahan pengkodean dalam sistem kontrol akses. Kesalahan ini, yang tidak terdeteksi selama empat tahun, memungkinkan peretas untuk menghindari langkah-langkah keamanan dan mengakses data sensitif.

CEO sementara Optus Michael Venter mengakui pelanggaran itu, mengatakan bahwa itu disebabkan oleh kerentanan yang sebelumnya tidak diketahui dalam pertahanan mereka yang timbul dari kesalahan pengkodean historis. Dia menekankan bahwa serangan itu dilakukan oleh penjahat yang termotivasi dan tegas yang memanfaatkan kerentanan dengan meniru aktivitas pelanggan biasa dan berputar melalui puluhan ribu alamat IP yang berbeda untuk menghindari deteksi.

Pelanggaran ini menyebabkan publikasi data sensitif di web gelap, dengan peretas menuntut tebusan A $ 1,5 juta dalam *cryptocurrency*. Namun, para peretas kemudian mengklaim telah menghapus semua data, dan tidak ada tebusan yang dibayar.[8] Pelanggaran data Optus telah menimbulkan kritik yang signifikan dan menyerukan langkah-langkah keamanan siber yang lebih baik di Australia. Pemerintah Australia telah mengakui bahwa negara ini tertinggal di belakang negara-negara maju lainnya dalam hal keamanan siber dan privasi data, dan pelanggaran tersebut telah menyoroti kebutuhan untuk peraturan yang lebih kuat dan perlindungan data pelanggan yang lebih baik.

Optus telah mengambil langkah- langkah untuk mengatasi kerentanan dan meningkatkan pertahanan keamanan siber. Perusahaan juga telah mengembalikan 20.071 pelanggan untuk biaya penggantian dokumen identitas dan membayar biaya yang dialami oleh lembaga pemerintah. Saat ini kasus tersebut berada di Pengadilan Federal, dengan ACMA mencari hukuman sipil terhadap Optus karena dugaan gagal melindungi data pelanggan. Optus berniat untuk membela tuduhan dan memperbaiki catatan jika diperlukan.

Pemerintah Australia berjanji untuk meningkatkan pertahanan siber dengan anggaran sebesar 1,66 miliar dollar Australia dalam satu dekade ini. Ancaman siber tidak hanya berdampak pada keamanan nasional tetapi juga pada pertumbuhan ekonomi. Keamanan siber yang kuat dapat melindungi bisnis dari serangan siber yang dapat merusak reputasi dan merugikan pelanggan.

Strategi yang Diambil oleh Perdana Menteri Anthony Albanese

Antony Albanese, Perdana Menteri Australia, telah mengambil beberapa langkah dalam menghadapi *cyberwarfare* untuk melindungi infrastruktur digital Australia. Berikut beberapa kebijakan yang telah diambil:

1. *Security of Critical Infrastructure Act 2018* (SOCI Act).
   Merupakan kerangka kerja yang dirancang untuk mengawasi keamanan infrastruktur yang signifikan di Australia. Perubahan berturut-turut pada Undang- Undang SOCI mewajibkan entitas yang bertanggung jawab di sebelas sektor penting untuk memperkuat infrastruktur penting Australia.
   Pemerintah Australia telah memperluas Undang-Undang SOCI dengan mengeluarkan Undang-Undang Amendemen Legislasi Keamanan (Infrastruktur Kritis) 2021 (SLACI) yang mulai berlaku pada Desember 2021 dan Undang-Undang Amendemen Legislasi

Keamanan (Perlindungan Infrastruktur Kritis) 2022 (SLACIP) yang mulai berlaku pada April 2022. dalam upaya untuk meningkatkan kesiapan dan ketahanan infrastruktur penting negara.

2. *Australia's Cyber Security Strategy 2020*.
   Untuk meningkatkan kemampuan pemerintah dalam menghadapi serangan cyber, Undang-undang Keamanan Cyber Australia tahun 2019 telah diperbarui. Strategi Keamanan Cyber Australia 2023– 2030, yang dirilis pada November 2023. Undang-undang ini bertujuan untuk menjadikan Australia sebagai pemimpin dunia dalam keamanan siber pada tahun 2030. Undang-undang ini menetapkan enam "*cyber shields*" untuk melindungi warga negara dan perusahaan Australia dari ancaman *cyber*, dengan masing-masing memberikan lapisan pertahanan tambahan, menjadikan Australia lebih sulit untuk diserang. *Cyber Shields* tersebut yaitu:

   a) *Strong Businesses And Citizens*: Memberdayakan individu dan bisnis untuk menjadi lebih sadar cyber dan resilien.
   b) *Safe technology*: Promosi pengembangan dan penggunaan teknologi yang aman.
   c) *World-Class Threat Sharing And Blocking*: Meningkatkan kolaborasi dan berbagi informasi untuk lebih baik mengidentifikasi dan memblokir ancaman *cyber*.
   d) *Protected Critical Infrastructure*: Memperkuat keamanan siber infrastruktur kritis seperti energi dan sistem perawatan kesehatan.
   e) *Sovereign Capabilities*: Mengembangkan keahlian dan teknologi *cybersecurity* Australia sendiri.
   f) *Resilient Region And Global Leadership*: Bekerja sama dengan mitra regional dan internasional untuk meningkatkan keamanan siber global.

3. *Australian Cyber Security Centre* (ACSC).
   Australian Cyber Security Centre (ACSC) merupakan badan pemerintah Australia yang bertanggung jawab untuk meningkatkan keamanan siber nasional. ACSC adalah bagian dari *Australian Signals Directorate* (ASD) dan didirikan pada tahun 2018.
   Pemerintah Australia telah mendirikan *Australian Cyber Security Centre* (ACSC) sebagai pusat koordinasi keamanan siber nasional. ACSC yang bertugas dalam mendorong pertukaran data, meningkatkan kesadaran akan ancaman dunia maya, dan mengurangi ancaman keamanan yang terkait dengan adopsi teknologi dan layanan baru.
   Kegiatan ACSC diatur oleh undang-undang dan kebijakan seperti Undang-Undang Polisi Federal Australia 1979, Undang- Undang Layanan Intelijen 2001, Undang- Undang Komisi Kejahatan Australia 2002, dan Undang-Undang Organisasi Intelijen Keamanan Australia 1979.
   ACSC *Research Fund***,** menyediakan dana penelitian kompetitif untuk mendukung proyek-proyek R&D keamanan siber yang berfokus pada bidang prioritas nasional. Program ini memberikan dukungan finansial kepada para peneliti di universitas, lembaga riset, dan perusahaan rintisan untuk mengembangkan solusi inovatif di bidang keamanan siber.

ACSC Cyber Challenges, ACSC yang menyelenggarakan kompetisi dan tantangan keamanan siber untuk mendorong para peneliti dan developer muda untuk menciptakan solusi inovatif. Berperan penting dalam memastikan hasil penelitian R&D keamanan siber dapat diimplementasikan secara efektif.

4. *Cyber Security Cooperation Program*.

   Pemerintah Australia telah mengembangkan program kerjasama keamanan *cyber* dengan negara-negara lain, termasuk Amerika Serikat, Kanada, dan Australia. Tujuan dari program ini adalah untuk meningkatkan kerjasama antar- negara dalam menghadapi ancaman siber dan meningkatkan kemampuan deteksi dan tanggapan terhadap serangan siber.

   Cyber Cooperation Program, program yang mencakup berbagai inisiatif untuk meningkatkan kemampuan dalam mendeteksi dan merespons serangan siber secara efektif. Program ini bertujuan memperkuat pertahanan siber suatu negara atau organisasi dengan membangun kapasitas manajemen insiden, pengembangan strategi nasional, serta pertukaran informasi terkait ancaman dan serangan siber. Program ini juga didukung oleh kebijakan dan strategi nasional serta kerangka kerja internasional yang mengatur tata kelola keamanan siber, seperti ASEAN *Cybersecurity Cooperation Strategy* (ACCS) yang membantu koordinasi dan sinergi antarnegara anggota ASEAN dalam menangani kejahatan dan ancaman siber.

   *Cyber and Critical Tech Cooperation Program***,** Australia bekerja dengan mitra regional dalam Program Kerja Sama Teknologi Siber dan Teknologi Kritis untuk meningkatkan ketahanan siber dan teknologi kritis di seluruh Indo-Pasifik. Program ini membantu Australia memperkuat kapasitas untuk memaksimalkan peluang dan mengurangi risiko yang terkait dengan penggunaan ruang siber dan teknologi kritis. Untuk proyek pengembangan kapasitas siber dan teknologi kritis di kawasan Indo-Pasifik, calon mitra diundang untuk mengajukan konsep melalui penawaran terbuka program. Dalam upayanya untuk mencapai hasil Program dengan bermitra dengan mitra baru dan berkolaborasi dengan berbagai industri, Program Panggilan Terbuka bertujuan untuk mencari dan mencoba metode baru dan inventif.

5. *Cyber Security Research and Development.*

   Pemerintah Australia telah meningkatkan investasi dalam penelitian dan pengembangan keamanan siber guna meningkatkan kemampuan melindungi infrastruktur digital negara dan meningkatkan deteksi dan tanggapan terhadap serangan siber. Berikut ini adalah beberapa contoh inisiatif dan organisasi di Australia yang berfokus pada penelitian dan pengembangan keamanan siber:

   a) *Advanced Cyber Security Engineering Research Centre(ACSRC)- University of Newcastle***.** Berkonsentrasi pada pembuatan model dan metode yang akan memungkinkan sistem komputer yang aman dan dapat diandalkan. *Cloud Security,*

Secure Virtualization, dan *Security of Internet of Things* adalah beberapa topik yang mereka pelajari.

b) *Deakin Cyber Research and Innovation Centre*: mengembangkan metode dan teknologi baru untuk melindungi internet di Australia dan di luar negeri. Mereka bekerja sama dengan Tata Consulting Services (TCS), CSIRO/Data 61, dan *Cyber Security Cooperative Research Centre* untuk mengembangkan teknologi autentikasi generasi berikutnya yang akan melindungi aset dalam infrastruktur penting seperti energi, pertahanan, transportasi, dan ruang angkasa.

c) *Centre for Cyber Security Research and Innovation (CCSRI) - RMIT University*: sebuah pusat penelitian yang mengembangkan penelitian yang memiliki rigor akademis dan hasil yang dapat diterapkan untuk meningkatkan kemampuan keamanan siber. Mereka bekerja sama dengan pihak industri dan universitas untuk mengembangkan pendekatan multi-disipliner dan berbasis aplikasi.

Kesimpulan

Cyberwarfare adalah penggunaan serangan siber oleh negara atau organisasi internasional untuk menyerang dan merusak jaringan komputer atau informasi nnegara lain. Ini berbeda dengan perang siber, di mana *cyberwarfare* mencakup teknik, taktik, dan prosedur yang mungkin terlibat dalam perang dunia maya, dan perang siber menggambarkan periode serangan siber yang berlarut-larut, termasuk dalam kombinasi dengan aksi militer tradisional.

Upaya yang telah dilakukan oleh Perdana Menteri Albanese antara lain; *Act of Critical Infrastructure Security 2018* (SOCI Act): Meningkatkan keamanan infrastruktur yang penting; *Australian Cyber Security Centre* (ACSC): Meningkatkan keamanan siber nasional; *Australia's Cyber Security Strategy 2020*: Meningkatkan kemampuan pemerintah dalam menghadapi serangan siber; *Cyber Security Cooperation Program*: Meningkatkan kerja sama internasional dalam memerangi *cyberwarfare*; *Cyber Security Research and Development*: Meningkatkan investasi dalam penelitian dan pengembangan keamanan siber. Meskipun sudah beberapa langkah yang telah diambil oleh pemerintah Australia untuk meningkatkan pertahanan siber negaranya, masih perlu banyak hal yang harus dilakukan untuk melindungi keamanan infrastruktur digital Australia.

Referensi

Buku:

Green, J.A. (Ed.). (2015). Cyber Warfare: A Multidisciplinary Analysis (1st ed.). Routledge. https://doi.org/10.4324/978131576 1565

Kestner, P. (2024). *The Art of Cyber Warfare: Strategic and Tactical Approaches for Attack and Defense in the Digital Age*. Springer Nature.

Whyte, C., & Mazanec, B. (2023). Understanding Cyber-Warfare: Politics, Policy and Strategy

(2nd ed.). Routledge. https://doi.org/10.4324/978100324 6398

Jurnal:

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *119*, 102754.

Ali, O., Shrestha, A., Chatfield, A., & Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly*, *37*(1), 101419.

Atrews, R. A. (2020). Cyberwarfare. *Journal of Information Warfare*, *19*(4), 17-28.

Bongiovanni, I., Renaud, K., & Cairns, G. (2020). Securing intellectual capital: an exploratory study in Australian universities. *Journal of Intellectual Capital*, *21*(3), 481-505.

Dupont, B., & Whelan, C. (2021). Enhancing relationships between criminology and cybersecurity. *Journal of criminology*, *54*(1), 76-92.

Khoirunnisa, Silvi, M., & Surya, E. A. R. (2024). Implementation of Cyberspace Cooperation between Indonesia and United States A Combating Cyberterrorism in Indonesia, 2019–2023. *Ilomata International Journal of Social Science*, *5*(3), 660-678. https://doi.org/10.61194/ijss.v5i3. 1173

Weil, T., & Murugesan, S. (2020). IT risk and resilience—Cybersecurity response to COVID-19. *IT professional*, *22*(3), 4-10.

Publikasi Umum:

Brodtmann, G., Caples, A., Cave, D., & Keast, J. (2023). *What Do Australia's Parliamentarians Think about Cybersecurity and Critical Technology?*. Australian Strategic Policy Institute.

M. Rafly, Ramadhan (2023). Skripsi: *ANALISIS KEBIJAKAN SIBER INDONESIA TERKAIT ASEAN CYBERSECURITY COOPERATION STRATEGY (ACCS) TAHUN 2019 – 2022.*

Website:

Almaata.ac.id. 2023. 23 Jenis Serangan Cybersecurity. 23 JENIS SERANGAN CYBERSECURITY - Fakultas Ilmu-IlmuKesehatan (almaata.ac.id) diakses pada 03 Juli 2025, pukul 13:57 WIB

Australian Goverment. 2023. 2023-0030 Australian Cyber Security Strategy. 2023-2030 Australian Cyber Security Strategy (homeaffairs.gov.au) Diakses pada 03 Juli 2025 pukul 20:06 WIB

Defence.gov.au. 2023. Release of the Annual Cyber Theat Report 2022- 2023. Rilis Laporan Ancaman Siber tahunan 2022-23 | Menteri Pertahanan (defence.gov.au) diakses pada tanggal 03 Juli 2025, pukul 23:54 WIB

Dfat.gov.au. 2021. Cyber and Critical Tech Coopertion Program: standing Open Call for

Proposals. Cyber and Critical Tech Cooperation Program: Standing Open Call for Proposals | Australian Government Department of Foreign Affairs and Trade (dfat.gov.au) diakses pada 03 Juli 2025, pukul 21:24 WIB

Directory. 2024. Australian Cyber Security Centre. Australian Cyber Security Centre | Directory diakses pada 03 Juli 2025, pukul 14:58 WIB

Dqsglobal. 2023. Manajemen Kerentanan dalan konteks ISO 27001. Manajemen kerentanan dalam konteks ISO 27001 - DQS (dqsglobal.com) diakses pada 03 Juli 2025, pukul 14:30 WIB

Energy Magazine. 2021. Critical Infrastructur Reform-Are you ready?. Critical Infrastructure Reform – Are you ready? - Energy Magazine diakses pada pada 03 Juli 2025, pukul 20:57 WIB

ITnews. 2024. Optus Breach allegedly Enable by Access Control Coding Eror. Optus breach allegedly enabled by access control coding error - Security - Telco/ISP - iTnews diakses pada 03 Juli 2025, pukul 20:57 WIB

Kompas.id. 2021. Serangan Siber di Australia Meningkat, Layanan Penting Diincar. Serangan Siber di Australia Meningkat, Layanan Penting Diincar - Kompas.id Diakses pada pada 03 Juli 2025, pukul 14:10 WIB

KpmgAustralia. SOCI| Critical Infrastructur assets protection. SOCI Act | Critical infrastructure assets protection - KPMG Australia diakses pada 03 Juli 2025, pukul 14: 20 WIB

UpGuard. 2024. 13 Biggest Data breaches in Australia. 13 Biggest Data Breaches in Australia [Updated 2024] | UpGuard diakses pada 03 Juli 2025, pukul 14:42 WI