LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

OPTIMALISASI INFRASTRUKTUR SIBER GUNA MELINDUNGI KEAMANAN NASIONAL AUSTRALIA

Oleh :

Jessica Kerr, B.P.S., M.A.
Departement Pertahanan Australia

KERTAS KARYA ILMIAH PERORANGAN (TASKAP)
PROGRAM PENDIDIKAN REGULER ANGKATAN (PPRA) LXVI
LEMBAGA KETAHANAN NASIONAL RI
TAHUN 2024

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

KATA PENGANTAR

Assalamualaikum Wr. Wb., salam sejahtera bagi kita semua.

Dengan memanjatkan puji syukur kehadirat Tuhan Yang Maha Esa serta atas segala rahmat dan karunia-Nya, penulis sebagai salah satu peserta Program Pendidikan Reguler Angkatan (PPRA) LXVI telah berhasil menyelesaikan tugas dari Lembaga Ketahanan Nasional Republik Indonesia sebuah Kertas Karya Ilmiah Perseorangan (Taskap) dengan judul *"Optimalisasi Infrastruktur Siber Guna Melindungi Keamanan Nasional Australia"*.

Penentuan Tutor dan judul Taskap ini didasarkan oleh Keputusan Gubernur Lembaga Ketahanan Nasional Republik Indonesia Nomor 71 Tahun 2024 tanggal 28 Maret 2024 tentang Pengangkatan Tutor Taskap kepada para peserta PPRA untuk menulis Taskap dengan memilih judul yang telah ditentukan oleh Lemhannas RI.

Pada kesempatan ini, perkenankanlah penulis menyampaikan ucapan terima kasih kepada Bapak Gubernur Lemhannas RI yang telah memberikan kesempatan kepada penulis untuk mengikuti PPRA LXVI di Lemhannas RI tahun 2024. Ucapan yang sama juga disampaikan kepada Tutor Taskap kami yaitu Mayjen TNI (Purn). Abdul Chasib dan Tim Penguji Taskap serta semua pihak yang telah membantu serta membimbing Taskap ini sampai terselesaikan sesuai waktu dan ketentuan yang dikeluarkan oleh Lemhannas RI.

Penulis menyadari bahwa kualitas Taskap ini masih jauh dari kesempurnaan akademis, oleh karena itu dengan segala kerendahan hati mohon adanya masukan guna penyempurnaan naskah ini.

Besar harapan saya agar Taskap ini dapat bermanfaat sebagai sumbangan pemikiran penulis kepada Lemhannas RI, termasuk bagi siapa saja yang membutuhkannya.

Semoga Tuhan Yang Maha Esa senantiasa memberikan berkah dan bimbingan kepada kita semua dalam melaksakan tugas dan pengabdian kepada Negara dan Bangsa yang kita cintai dan kita banggakan.

Sekian dan terima kasih. Wassalaamualaikum Wr. Wb.

Jakarta, 19 Augustus 2024
Penulis,

Jessica Kerr

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

PERNYATAAN KEASLIAN

1. Yang bertanda tangan di bawah ini:

   Nama : Jessica Kerr
   Pangkat : -
   Jabatan : Direktor Strategi
   Instansi : Departmen Pertahanan Australia
   Alamat : Jl K.H. Wahid Hasim No.110-112, Kb. Sirih, Kec. Menteng, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10340

   Sebagai peserta Program Pendidikan Reguler Angkatan (PPRA) ke LXVI tahun 2024 menyatakan dengan sebenarnya bahwa:

   a. Kertas Karya Ilmiah Perseorangan (Taskap) yang saya tulis adalah asli.
   b. Apabila ternyata sebagian atau seluruhnya tulisan Taskap ini terbukti tidak asli atau plagiasi, maka saya bersedia untuk dibatalkan.

2. Demikian pernyataan keaslian ini dibuat untuk dapat digunakan seperlunya.

Jakarta, 19 Augustus 2024
Penulis,

Jessica Kerr

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

DAFTAR ISI

Halaman

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1. Latar Belakang

Sejalan dengan tren global, infrastruktur siber dan sistem digital Australia menjadi semakin kompleks dan saling bergantung. Dapat dikatakan bahwa seluruh aspek kehidupan sehari-hari di Australia didukung oleh konektivitas digital – mulai dari perbankan, transportasi, hingga komunikasi. Pesatnya digitalisasi kehidupan sehari-hari yang terjadi selama tiga puluh tahun terakhir telah membawa banyak manfaat bagi masyarakat Australia, termasuk kemakmuran ekonomi, peluang komersial, dan penyediaan layanan pemerintah yang lebih efisien. Namun, peluang ini datang bersamaan dengan semakin menantangnya risiko siber yang mempunyai potensi dampak serius terhadap keamanan nasional.

Serangan siber dapat diluncurkan dari mana saja di dunia dan dunia maya tidak mengikuti batas-batas geografis tradisional negara. Pelaku ancaman siber dapat menargetkan apa pun yang terhubung atau ada di internet, termasuk peralatan elektronik, informasi, dan sumber daya keuangan. Seiring dengan berkembangnya infrastruktur siber di Australia, luasnya 'ruang serangan siber' (*cyber attack surface*) juga meningkat, yaitu jumlah titik di mana pelaku ancaman dapat mencoba masuk, menimbulkan dampak, atau mengambil data.[1] Jika tidak dikelola dengan hati-hati, infrastruktur siber Australia akan semakin rentan terhadap serangan.

Bidang keamanan siber bersifat dinamis, dan berkembang seiring dengan pesatnya kemajuan teknologi baru. Perkembangan teknologi telah menghasilkan alat dan metode serangan yang semakin canggih yang dapat dimanfaatkan oleh pelaku ancaman siber untuk menyusup ke infrastruktur siber Australia. Misalnya, teknologi memungkinkan pelaku ancaman siber untuk: beroperasi secara anonim dari perspektif identitas dan lokasi; mengenkripsi aktivitas mereka sehingga lebih

[1] National Institute of Standards and Technology. *NIST Computer Security Resource Centre*. https://csrc.nist.gov/glossary/term/attack_surface#:~:text=attack%20surface%20Definitions%3A%20The%20set%20of%20points%20on,data%20from%2C%20that%20system%2C%20system%20element%2C%20or%20environment.

sulit dideteksi; lebih mudah mengkompromikan sistem digital; mengotomatiskan serangan; meniru situs web yang sah; dan memanfaatkan AI, antara lain.

Pemerintah Australia mendefinisikan pelaku ancaman siber sebagai individu atau organisasi yang melakukan aktivitas jahat, seperti spionase siber, serangan siber, atau kejahatan yang dimungkinkan oleh dunia maya.[2] Pelaku ancaman siber dan motivasi mereka biasanya dapat dimasukkan ke dalam empat kategori: penjahat siber terorganisir (biasanya dimotivasi oleh keuntungan finansial); aktivis atau kelompok yang dimotivasi isu (yang mengganggu organisasi untuk menyoroti suatu tujuan); negara, atau pelaku yang disponsori negara (spionase, pencurian, atau aktivitas mengganggu lainnya yang memajukan kepentingan negara itu); dan ancaman orang dalam (akses terhadap informasi). Yang menyatukan semua ancaman pelaku siber di atas adalah kemampuan dan niat untuk merusak atau membahayakan infrastruktur atau data siber demi keuntungan yang dirasakan. Tindakan-tindakan ini, apa pun motivasinya, berpotensi membahayakan infrastruktur penting, menimbulkan ketidakpercayaan terhadap pemerintah Australia, dan mengganggu keamanan nasional Australia.

Infrastruktur siber Australia belum dioptimalkan untuk mencegah dan menanggapi ancaman siber. Australia memiliki infrastruktur siber yang relatif matang. Misalnya: *Australian Cyber Security Centre* (ACSC, Pusat Keamanan Siber Australia), yang didirikan pada tahun 2014, merupakan badan utama Pemerintah untuk keamanan siber; jabatan Menteri Keamanan Siber ditetapkan kembali pada tahun 2022 dan diangkat menjadi anggotta kabinet; dan strategi keamanan siber Australia yang baru dirilis pada tahun 2023. Meskipun demikian, masih ada kekurangan dalam pendekatan Australia terhadap keamanan siber. Misalnya: anggaran dan prioritas yang diberikan pada keamanan siber berubah dari satu Pemerintah ke Pemerintah lainnya; meskipun ACSC merupakan lembaga siber utama pemerintah, tanggung jawab atas isu-isu siber ditanggung bersama oleh beberapa departemen pemerintah yang berbeda, sehingga menimbulkan ketidakjelasan garis tanggung jawab dan tidak optimalnya sinergi antar pemangku kepentingan; ada kekurangan standar dan peraturan wajib; dan

[2] Australian Signals Directorate. *Australian Cyber Security Centre Glossary*. https://cyber.gov.au/glossary/threat-actor

kurangnya tenaga kerja terampil di dunia maya. Seperti akan diuraikan dalam taskap ini, kekurangan dalam infrastruktur siber saat ini mempunyai implikasi potensial terhadap keamanan nasional. Perlu dioptimalkan regulasi, tata kelola, sumber daya manusia, teknis dan kerja sama domestik dan internasional.

Belum optimalnya infrastruktur siber Australia terlihat dari meningkatnya jumlah dan tingkat keparahan serangan siber yang dialami. Pada periode Juni 2022 – Juli 2023 hampir 94.000 kejadian kejahatan siber dilaporkan ke ACSC, dengan rata-rata satu laporan setiap enam menit. [3] Jumlah ini meningkat sebesar 23 persen dari periode pelaporan sebelumnya. Biaya rata-rata kejahatan siber per laporan juga meningkat sebesar 14 persen pada tahun 2021-2022. Laporan tersebut mencatat bahwa pada periode Juni 2022 – Juli 2023 *Australian Signals Directorate* (ASD, Direktorat Sinyal Australia) menanggapi 143 kejadian siber terkait infrastruktur penting nasional, meningkat dari 95 kejadian pada tahun sebelumnya. Perlu dioptimalkan infrastruktur siber Australia termasuk

Pada akhir tahun 2022, warga negara Australia menjadi korban tiga serangan siber besar-besaran terhadap Medibank (perusahaan asuransi kesehatan swasta), Optus (perusahaan telekomunikasi), dan Latitude (layanan keuangan) yang berdampak pada lebih dari 30 juta akun. Meskipun data mengenai serangan siber terhadap lembaga pemerintah Australia lebih sulit ditemukan, Laporan Intelijen Ancaman Global BlackBerry (2023) menyoroti bahwa *Blackberry Cyber Security Solutions* menghentikan lebih dari 55.000 serangan terhadap pemerintah dan sektor layanan publik secara global, dengan Australia sebagai salah satu negara yang menjadi sasaran utama serangan siber di kawasan Asia-Pasifik.[4]

Domain digital menyediakan saluran bagi musuh potensial untuk melakukan serangan terhadap suatu negara atau kepentingan negara dengan cara yang lebih murah dan lebih terselubung dibandingkan serangan fisik tradisional. Aktivitas siber yang berbahaya berpotensi berdampak pada keamanan nasional dalam

---

[3] Australian Signals Directorate (2023), *Cyber Threat Report 2022-23.* https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf

[4] Blackberry (2023). *Global Threat Intelligence Report.* https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/bbcomv4/blackberry-com/en/solutions/threat-intelligence/2023/ laporan-ancaman-intelijen-agustus/Blackberry-Global-Ancaman-Laporan-Intelijen-Agustus-2023.pdf

beberapa cara, termasuk memungkinkan akses terhadap informasi keamanan rahasia, ancaman stabilitas ekonomi, mengganggu rantai pasokan, dan menolak atau menurunkan akses infrastruktur penting (telekomunikasi, kesehatan, dll). Oleh karena itu penting untuk menganalisis keamanan siber dari sudut pandang dampaknya terhadap keamanan nasional.

2. Rumusan Masalah

Berdasarkan uraian latar belakang serta fakta dan kondisi yang terjadi, dapat dikatakan terdapat kesenjangan antara infrastruktur di Australia saat ini dan dapat disebut belum optimal untuk menanggapi ancaman saat ini dan di masa depan secara efektif. Australia sudah dianggap sebagai salah satu negara paling aman secara siber di dunia. Australia berada di peringkat ke-12 dalam Indeks Keamanan Siber Global dan peringkat ke-3 dalam Indeks Keamanan Siber Nasional.[5][6] Namun demikian, infrastruktur siber Australia masih bisa dioptimalisasi. Pada kenyataannya, ancaman siber yang dihadapi oleh negara-negara di dunia, termasuk Australia, terus tumbuh dan berkembang dengan pesat. Respons harus tetap tangkas, dengan mempertimbangkan siklus evolusi dan optimalisasi yang berkelanjutan untuk mengimbangi ancaman. Risiko kalau tidak adanya tindakan sangatlah besar. Serangan siber berpotensi berdampak pada seluruh aspek kehidupan di Australia:

a. **Politik:** Dampak serangan siber dan kampanye misinformasi dapat melemahkan kepercayaan publik terhadap integritas proses pemilu dan pemerintahan. Aktivitas siber yang berbahaya dapat menyebabkan meningkatnya polarisasi politik dan mengancam kohesi sosial. Terjadinya serangan siber dapat meningkatkan kecemasan masyarakat bahwa institusi pemerintah tidak mampu melindungi atau memberikan keamanan kepada mereka.

b. **Ekonomi:** Dampak ekonomi dari serangan siber mencakup kerugian finansial signifikan yang terkait dengan kejahatan siber, serta biaya untuk

---

[5] International Telecommunications Union (2021), *Global Cyber Security Index 2020*. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[6] e-Governance Academy Foundation (2024), *National Cyber Security Index.* https://ncsi.ega.ee/ncsi-index/?order=rank&type=c

mempertahankan langkah-langkah keamanan siber yang tepat untuk mencegah serangan. Menurut *World Economic Forum*, kerugian global akibat kejahatan siber diperkirakan akan mencapai USD 23,84 triliun pada tahun 2027, naik dari USD 8,44 triliun pada tahun 2022 dan USD 0,86 triliun pada tahun 2018.[7]

c. Sosial: Kejahatan siber pada tingkat individu dan bisnis dapat mengakibatkan kerugian finansial yang signifikan dan rusaknya reputasi. Di tingkat masyarakat, aktivitas siber yang berbahaya dapat menyebabkan meningkatnya polarisasi dan mengancam kohesi sosial dengan memperbesar perpecahan. Aktivitas siber yang berbahaya juga dapat mengancam infrastruktur penting, termasuk kesehatan, listrik, dan jaringan telekomunikasi yang penting bagi keberfungsian masyarakat.

d. Teknologi: Kemajuan pesat dalam teknologi membawa peluang sekaligus tantangan, meningkatkan deteksi dan respons ancaman, namun juga memungkinkan serangan siber yang lebih maju dan canggih. Ketika ketergantungan pada teknologi meningkat, peluang untuk melakukan kejahatan siber pun meningkat secara eksponensial.

Kaitan antara kejahatan siber dan keamanan nasional menjadi semakin lazim seiring dengan kemajuan teknologi yang meningkatkan kemampuan pelaku kejahatan untuk menimbulkan kerugian. Tidak perlu lagi ada invasi fisik atau militer untuk adanya ancaman terhadap keamanan dalam negeri seperti kesehatan, ekonomi atau kohesi sosial. Ancaman-ancaman seperti ini mempunyai implikasi penting bagi keamanan nasional karena potensi gangguan atau kerugian yang signifikan terhadap masyarakat Australia. Maka perlu dipertimbangkan lebih lanjut mengenai optimalisasi infrastruktur untuk melindungi keamanan nasional Australia. Oleh karena itu, rumusan masalah yang akan dibahas dalam Taskap ini adalah ***'Bagaimana mengoptimalkan infrastruktur siber guna melindungi keamanan nasional Australia?'***

Dalam rangka menjawab dan menemukan solusi atas permasalahan yang

[7] World Economic Forum (2024). *2023 Was a Big Year For Cybercrime – Here's How We Can Make Our Systems Safer* https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety/

telah dijelaskan pada Rumusan Masalah, maka pertanyaan penelitian yang akan dibahas dalam Taskap ini antara lain sebagai berikut:

a. Bagaimana pentingnya membangun infrastruktur siber yangmendukung keamanan?
b. Bagaimana pengaruh regulasi terhadap infrastruktur siber?
c. Apa dampaknya infrastruktur siber terhadap keamanan nasional?
d. Bagaimana strategi mengoptimalkan infrastruktur siber guna melindungi keamanan nasional?

3. Maksud dan Tujuan.

a. Maksud dari penulisan ini adalah untuk memberikan kontribusi terkait kumpulan pengetahuan tentang hubungan antara keamanan siber dan keamanan nasional dan memberikan analisis strategis tentang bagaimana infrastruktur keamanan siber Australia dapat dioptimalkan untuk melindungi keamanan nasional Australia dari ancaman siber.

b. Tujuan dari penulisan ini adalah untuk memberikan rekomendasi praktis kepada para pembuat kebijakan dan pengambil keputusan di pemerintahan Australia dan untuk memberikan wawasan berharga yang tidak hanya mengatasi tantangan saat ini tetapi juga meletakkan landasan bagi pendekatan masa depan yang adaptif.

4. Ruang Lingkup dan Sistematika.

a. Ruang Lingkup: Agar rumusannya lebih jelas maka penulis membatasi ruang lingkup pembahasan pada infrastruktur siber di Australia. Meskipun diskusinya fokus pada Australia, Taskap ini akan mempertimbangkan bagaimana lingkungan internasional berdampak pada kondisi di Australia. Taskap ini fokus secara khusus pada pengalaman dan peluang bagi pemerintah dan dunia usaha. Meskipun individu menghadapi ancaman keamanan siber, dampak dari aktivitas jahat pada tingkat ini kecil kemungkinannya menimbulkan konsekuensi keamanan nasional yang berarti, maka Taskap ini tidak akan mengkaji isu-isu yang berkaitan dengan individu. Untuk lebih menyempurnakan fokus tersebut, Taskap ini akan fokus

pada solusi yang dapat diterapkan oleh pemerintah. Negara mempunyai tanggung jawab utama atas keamanan nasional wilayahnya – termasuk serangan siber yang mungkin terjadi di wilayahnya – sehingga solusi yang dipimpin oleh pemerintah akan memberikan respons yang paling efektif.

b. Sistematika Penulisan: Taskap ini akan diatur dengan sistematika sebagai berikut:

1) **Bab I – Pendahuluan.** Bab ini memberikan gambaran tentang latar belakang yang relevan, menjelaskan rumusan masalah, maksud dan tujuan, ruang lingkup dan sistematika, serta metode dan pendekatan. Definisi istilah-istilah penting yang akan digunakan dalam Taskap ini juga disediakan.

2) **Bab II – Landasan Pemikiran.** Bab ini memberikan landasan teoritis dan lingkungan strategis untuk pembahasan permasalahan yang diangkat. Bab ini akan mulai dengan penjelasan kerangka hukum dan peraturan yang mendukung keamanan siber Australia. Kemudian akan menguraikan strategi keamanan siber dan strategi pertahanan nasional pemerintah Australia sebagai ekspresi publik atas pendekatan Australia saat ini terhadap keamanan siber. Bab ini akan memperkenalkan teori-teori inti yang akan digunakan dalam Taskap ini untuk memberikan kerangka dan dasar logis untuk analisis selanjutnya. Terakhir, bab ini akan memberikan analisis terhadap lingkungan strategis nasional, regional, dan internasional terkait keamanan siber dalam konteks keamanan nasional.

3) **Bab III – Pembahasan.** Bab ini akan membahas masing-masing pertanyaan penelitian yang dihubungkan dengan rumusan masalah. Bab ini ini akan menganalisis masalah secara sistematis untuk mengidentifikasi hambatan dan peluang serta mengusulkan pendekatan yang disarankan untuk memecahkan masalah. Bab ini akan merekomendasikan rencana aksi strategis yang spesifik, terukur, dapat ditindaklanjuti, relevan, dan terikat waktu untuk

mengoptimalkan infrastruktur siber Australia guna melindungi keamanan nasional Australia.

4) **Bab IV – Penutup.** Bab ini akan memberikan kesimpulan dan rekomendasi mengenai cara mengoptimalkan infrastruktur siber Australia untuk melindungi keamanan nasional Australia.

5. Metode dan Pendekatan

a. Metode: Taskap ini akan menggunakan metode analisis kualitatif-deskriptif dengan studi literatur dan data-data yang dikumpulkan dari berbagai sumber. Sumber ini termasuk tulisan akademisi, publikasi pemerintah dan dokumen lainnya.

b. Pendekatan: Pendekatan komprehensif dan holistik digunakan untuk menganalisis data dengan menggunakan perspektif keamanan nasional dan mempertimbangkan kerangka teori yang akan dijelaskan pada bab berikutnya.

6. Pengertian

a. Infrastruktur siber Merujuk pada kumpulan sistem dan perangkat lunak teknologi informasi, aset fisik dan informasi, proses, dan manusia yang memungkinkan suatu organisasi berfungsi secara efisien dan aman di dunia maya.[8] Hal ini juga mencakup kerangka kebijakan dan peraturan atau regulasi yang mendukung keamanan siber.

b. Keamanan nasional pada dasarnya adalah tentang melindungi suatu negara dari bahaya. Keamanan nasional adalah konsep inklusif yang mencakup ekonomi, masyarakat, keamanan sumber daya, tata kelola yang baik, dan ketahanan institusi.[9] Hal ini berkaitan dengan bagaimana suatu negara membentuk lingkungannya dan bagaimana negara tersebut

---

[8] Stewart, C (2010) 'What is Cyberinfrastructure'. *Proceedings of SIGUCCS 2010*. Norfolk, VA 24-27 October.

[9] Medcalf, R *The 2022 Order of Australia Lecture* (pidato, Australian National University, 7 Desember) https://www.anu.edu.au/news/all-news/making-sense-of-national-security

mencegah, mempersiapkan, dan merespons ancaman terhadap kedaulatan, masyarakat, aset, infrastruktur, dan institusi.[10]

c. Optimalisasi, menurut kamus Merriam-Webster adalah tindakan, proses, atau metodologi membuat sesuatu (seperti desain, sistem, atau keputusan) sebaik, sefungsional, atau seefektif mungkin.[11]

d. Keamanan siber adalah praktik melindungi jaringan, perangkat, dan data dari akses tidak sah atau penggunaan kriminal. Keamanan siber adalah teknologi, tindakan, atau praktik apa pun untuk mencegah serangan siber atau memitigasi dampaknya.[12]

e. Serangan siber adalah segala upaya yang disengaja untuk mencuri, mengubah, menonaktifkan, mengekspos, atau menghancurkan data, aplikasi, atau aset lainnya melalui akses tidak sah ke jaringan, sistem komputer, atau perangkat digital.[13]

f. Ancaman siber adalah keadaan atau peristiwa yang berpotensi memberikan dampak buruk terhadap operasi organisasi, aset organisasi, individu atau negara melalui sistem informasi menggunakan akses tidak sah, perusakan, pengungkapan, modifikasi informasi dan/atau penolakan layanan.[14]

g. Infrastruktur kritis/ infrastruktur penting adalah kumpulan sistem dan jaringan yang dianggap penting oleh pemerintah untuk berfungsinya masyarakat dan perekonomian sehari-hari. Pemerintah Australia mendefinisikan infrastruktur kritis sebagai "*fasilitas fisik, rantai pasokan, teknologi informasi dan jaringan komunikasi, yang jika dihancurkan, terdegradasi atau tidak tersedia untuk jangka waktu lama, akan berdampak signifikan terhadap kesejahteraan sosial atau ekonomi negara tersebut, atau mempengaruhi kemampuan Australia untuk menyelenggarakan pertahanan negara dan menjamin keamanan nasional*."[15]

---

[10] Commonwealth of Australia. *National Security Strategy*. Department of Prime Minister and Cabinet: Canberra. h.5
[11] Merriam-Webster. *Optimization*. https://www.merriam-webster.com/dictionary/optimization
[12] IBM (2022). *What is Cybersecurity*. https://www.ibm.com/topics/cybersecurity
[13] IBM (2022). *What is Cyber Action*. https://www.ibm.com/topics/cyber-action
[14] NIST. *Cyber Threat.* https://csrc.nist.gov/glossary/term/Cyber_Threat
[15] Cyber and Infrastructure Security Centre. *Security of Critical Infrastructure Act 2018*. https://www.cisc.gov.au/legislation-regulation-and-compliance/soci-act-2018

h. **Ransomware** adalah jenis perangkat lunak berbahaya yang mengenkripsi data korban, membuatnya tidak dapat diakses, dan meminta pembayaran tebusan untuk kunci dekripsi agar akses dapat dipulihkan.[16]

[16] IBM (2022). *What is Ransomware?* https://www.ibm.com/topics/ransomware

BAB II
LANDASAN PEMIKIRAN

7. Umum

Dalam mempertimbangkan titik temu antara keamanan siber dan keamanan nasional, pertama-tama harus memahami pengaruh faktor lingkungan, serta menetapkan kerangka teoritis untuk memandu analisis. Bab ini akan dimulai dengan menguraikan peraturan, perundang-undangan dan strategi yang saat ini memandu pendekatan Australia terhadap keamanan siber. Selanjutnya akan dikaji data dan fakta yang relevan untuk memberikan pemahaman yang lebih mendalam kepada pembaca mengenai skala dan ruang lingkup permasalahan yang sedang dibahas. Bab ini akan memaparkan teori-teori yang relevan guna membangun kerangka yang mendukung analisis selanjutnya. Terakhir, akan dibahas perkembangan lingkungan strategis nasional, regional dan internasional yang relevan dengan rumusan masalah.

8. Peraturan dan Perundang-undangan

a. Security *of Critical Infrastructure Act* 2018

Security of Critical Infrastructure Act (SOCI, *UU Keamanan Infrastruktur Penting*) tahun 2018 berupaya mengelola risiko keamanan nasional akibat sabotase, spionase, dan pemaksaan yang dilakukan oleh aktor asing dengan mendorong kesiapan dan ketahanan aset infrastruktur penting di Australia. Undang-undang ini bertujuan untuk meningkatkan keamanan siber di sebelas sektor penting perekonomian:

1) Komunikasi
2) Penyimpanan dan pemrosesan data
3) Industri pertahanan
4) Pendidikan tinggi dan penelitian
5) Energi
6) Jasa keuangan dan pasar
7) Makanan dan bahan makanan
8) Kesehatan dan medis
9) Teknologi luar angkasa
10) Angkutan

11) Air dan saluran pembuangan

UU SOCI diperkenalkan sebagai jawaban atas tantangan keamanan yang ditimbulkan oleh meningkatnya konektivitas infrastruktur penting Australia ke domain siber. Bagian 3(d) dari undang-undang tersebut mencakup penerapan kewajiban keamanan siber yang ditingkatkan pada entitas terkait 'untuk sistem yang mempunyai kepentingan nasional guna meningkatkan kesiapan dan kemampuan mereka dalam merespons insiden siber'.[17] UU SOCI menekankan pentingnya langkah-langkah keamanan yang kuat dan strategi manajemen risiko yang proaktif. Berdasarkan ketentuan yang diuraikan dalam Bagian 3(d), entitas diwajibkan untuk mematuhi standar kepatuhan yang ketat, yang mencakup melakukan audit keamanan rutin, menerapkan teknologi pertahanan siber yang canggih, dan berpartisipasi dalam program pelatihan berkelanjutan untuk staf mereka.

Selain itu, UU SOCI mengamanatkan pelaporan insiden secara *real-time* dan kolaborasi dengan otoritas keamanan siber nasional untuk memastikan respons yang terkoordinasi terhadap ancaman. Jika perusahaan yang bertanggung jawab atas aset infrastruktur penting mengetahui bahwa insiden keamanan siber telah terjadi atau sedang terjadi, dan insiden tersebut berdampak signifikan terhadap ketersediaan aset tersebut, maka insiden tersebut harus segera dilaporkan ke *Australian Cyber Security Centre* (ACSC) sedapat mungkin dan paling lambat 12 jam kemudian.[18] Pendekatan ini tidak hanya meningkatkan ketahanan infrastruktur penting terhadap potensi serangan siber namun juga menetapkan kerangka kerja untuk pemulihan yang cepat dan meminimalkan dampak terhadap keamanan nasional dan stabilitas ekonomi.

b. *Privacy Act* 1988

Di Australia, perlindungan data dan privasi pada prinsipnya diatur oleh *Privacy Act* (UU Privasi) tahun 1998. UU *Privacy* mewajibkan lembaga pemerintah federal Australia dan organisasi sektor swasta (dengan omset tahunan melebihi ambang batas yang ditentukan) untuk mengambil langkah-

[17] Commonwealth of Australia. *Security of Critical Infrastucture Act 2018*.
[18] *Ibid.* pasal 30BC(d)

langkah yang wajar untuk melindungi keamanan informasi tertentu dan untuk menghancurkan/memastikan de-identifikasi informasi pribadi jika tidak lagi diperlukan.[19] Persyaratan ini mencakup penerapan pengendalian fisik, administratif, dan teknis yang sesuai. Undang-undang tersebut juga menetapkan kondisi di mana informasi pribadi dapat dikumpulkan, digunakan, dan diungkapkan, memastikan transparansi dengan individu tentang bagaimana data mereka ditangani.

UU *Privacy* berisi 13 Prinsip Privasi Australia (PPA) yang menetapkan kewajiban entitas dalam pengelolaan informasi pribadi. Kepatuhan terhadap PPA mengurangi risiko pelanggaran data dengan mengurangi atau menghilangkan risiko privasi di setiap tahap siklus penanganan informasi pribadi (pengumpulan, penyimpanan, penggunaan, pengungkapan, penghancuran).[20] Organisasi wajib merespons pelanggaran privasi dengan cepat dan efektif, termasuk memberi tahu *Australian Information Commission* (Komisi Informasi Australia) dan individu yang terkena dampak ketika pelanggaran tersebut menimbulkan risiko kerugian serius. Pendekatan komprehensif ini bertujuan untuk menjunjung privasi sebagai hak mendasar sekaligus menyeimbangkan kebutuhan dunia usaha dan lembaga pemerintah untuk memproses data pribadi dalam kerangka yang diatur. Meskipun UU *Privacy* berlaku secara khusus untuk penanganan informasi pribadi, dalam praktiknya kepatuhan privasi yang kuat kemungkinan besar akan meningkatkan postur keamanan siber secara umum.

c. *Criminal Code Act* tahun 1995

Criminal Code Act (UU Kode Kriminal) 1995 memberikan kerangka hukum untuk menuntut berbagai bentuk pelanggaran digital. Undang-undang ini menargetkan individu dan kelompok yang terlibat dalam aktivitas yang membahayakan integritas, kerahasiaan, dan ketersediaan sistem dan jaringan komputer. Dengan mengkategorikan tindakan-tindakan ini sebagai tindak pidana, undang-undang ini berfungsi sebagai pencegah terhadap penjahat siber yang mungkin dan memberikan lembaga penegak hukum alat yang

[19] Commonwealth of Australia. *Privacy Act 1988* pasal 11
[20] *Ibid.*

diperlukan untuk menyelidiki dan mengadili kejahatan-kejahatan ini secara efektif.

Bagian 10.6 dan 10.7 UU tersebut memuat pelanggaran yang mengkriminalisasi penyalahgunaan jaringan telekomunikasi, 'layanan pengangkutan' (termasuk internet) dan komputer. Bagian 7.3, 10.6 dan 10.7 UU *Criminal Code* mencakup serangkaian pelanggaran komputer dan telekomunikasi yang mencakup:

1) memperoleh atau menangani informasi keuangan pribadi secara tidak jujur;
2) eksploitasi dan pelecehan seksual terhadap anak secara online;
3) penyalahgunaan dunia maya termasuk berbagi gambar intim tanpa persetujuan;
4) intrusi komputer;
5) modifikasi data tanpa izin, termasuk pemusnahan data;
6) gangguan yang tidak sah terhadap komunikasi elektronik, termasuk serangan penolakan layanan; dan
7) pembuatan dan distribusi perangkat lunak berbahaya (misalnya, virus dan ransomware).[21]

d. Strategi Keamanan Siber Pemerintah Australia

Pada tanggal 22 November 2023, Pemerintah Australia merilis *Australian Cyber Security Strategy 2023-2030* (ACSS, Strategi Keamanan Siber Australia), yang bertujuan untuk memperkuat pertahanan siber Australia guna mendukung ketahanan dan pemulihan cepat dari serangan siber. ACSS adalah strategi keamanan siber ketiga di Australia. Strategi pertama diluncurkan pada tahun 2016 dan berfokus pada peningkatan kemampuan siber pemerintah, menumbuhkan industri keamanan siber dalam negeri, dan membangun kapasitas penelitian dan pengembangan siber nasional. Sementara itu, strategi kedua, yang dirilis pada tahun 2020, berfokus pada perlindungan infrastruktur penting nasional dan meningkatkan kemampuan penegakan hukum dalam kaitannya dengan pemberantasan kejahatan siber.

[21] Commonwealth of Australia, *Criminal Code Act 1995*

ACSS berfokus pada enam 'perisai siber', sebuah metafora untuk pertahanan warga negara dan dunia usaha Australia dari ancaman siber:

1) **Dunia usaha dan masyarakat yang kuat**: meningkatkan kesadaran akan keamanan siber di kalangan masyarakat dan dunia usaha, meningkatkan pemahaman tentang ancaman siber dan tindakan yang dapat mereka ambil untuk melindungi diri mereka sendiri serta dukungan yang tersedia untuk memungkinkan pemulihan yang cepat setelah terjadinya pelanggaran.
2) **Teknologi yang aman:** akan menetapkan standar keamanan siber minimum untuk keamanan digital dalam produk, sehingga memerlukan penerapan keamanan optimal dalam pengembangan sejak awal. Perlindungan ini akan meningkatkan kepercayaan konsumen dan perusahaan bahwa produk digital yang dibeli di Australia aman digunakan.
3) **Pembagian dan pemblokiran ancaman kelas dunia**: mengusulkan pertukaran intelijen ancaman secara *real-time* antara pemerintah dan dunia usaha, sehingga memungkinkan ancaman diblokir sebelum menimbulkan kerugian bagi dunia usaha dan warga negara Australia.
4) **Infrastruktur penting yang dilindungi**: berfokus pada perlindungan infrastruktur penting dan membangun layanan yang andal termasuk air, energi, dan layanan kesehatan.
5) **Kemampuan berdaulat**: akan fokus pada pembangunan ekosistem siber yang berkembang dengan keterampilan siber yang tepat. Hal ini akan fokus pada pengembangan tenaga kerja siber, dan memastikan bahwa ini adalah profesi yang diinginkan oleh generasi muda.
6) **Kawasan yang berketahanan dan kepemimpinan global**: mengakui bahwa Australia lebih kuat ketika bekerja sama dengan tetangganya untuk memerangi ancaman siber global. Australia akan fokus pada peningkatan kemitraan global dan mendukung negara-

negara di kawasan yang kesulitan menghadapi lemahnya kontrol keamanan siber.[22]

ACSS adalah sebuah strategi ambisius yang berupaya mencapai visi Pemerintah untuk menjadi pemimpin dunia dalam keamanan siber pada tahun 2030. Namun, seperti yang akan dibahas pada bab berikutnya, terdapat tantangan dan kekurangan yang perlu diatasi agar infrastruktur siber optimal dapat benar-benar terwujud untuk menghadapi ancaman di masa depan dan melindungi keamanan nasional Australia.

e. Strategi Pertahanan Nasional

Strategi Pertahanan Nasional Australia tahun 2024 mencatat bahwa perkembangan di bidang ruang angkasa dan dunia maya berarti kepentingan keamanan Australia tidak terikat oleh geografi saja. *Australian Defence Force* (ADF) harus diintegrasikan di lima domain yaitu darat, maritim, udara, ruang angkasa, dan dunia maya untuk merespons lingkungan strategis saat ini. Pemerintah telah menetapkan bahwa ADF memerlukan peningkatan kemampuan siber untuk intelijen, pengawasan dan pengintaian, komunikasi yang tangguh, serta pertahanan dan gangguan jaringan komputer. Strategi Pertahanan Nasional mencatat bahwa kemampuan ruang angkasa dan dunia maya penting untuk melindungi keamanan nasional. Aktivitas siber yang berbahaya digunakan oleh negara untuk mengejar kepentingan mereka, termasuk melalui kampanye spionase dan disinformasi. Aktor-aktor negara dan non-negara sedang meningkatkan kemampuan siber mereka, sehingga meningkatkan risiko gangguan terhadap sistem, infrastruktur, dan jaringan penting di Australia.[23]

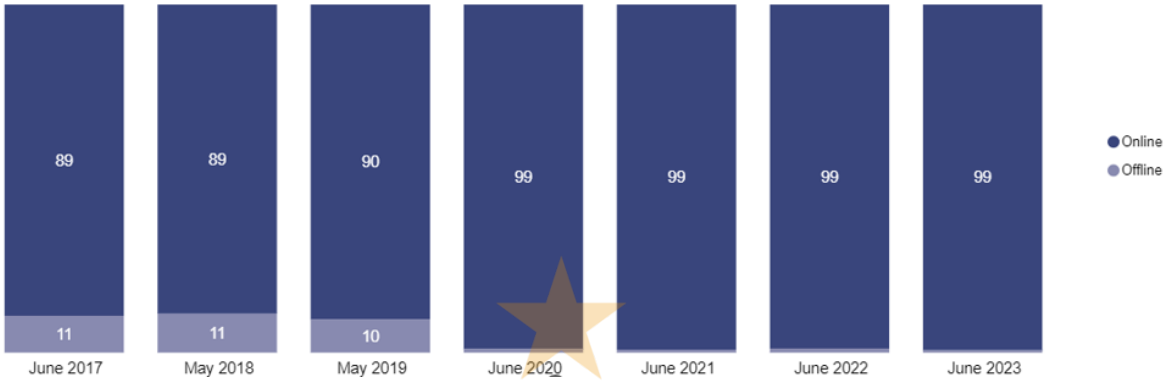
9. Data/fakta

a. Penggunaan internet di Australia

Hampir semua orang dewasa Australia memiliki akses ke internet, dan sebagian besar menggunakannya beberapa kali sehari. Dalam survei yang dilakukan oleh *Australian Media and Communications Authority (*Otoritas

[22] Commonwealth of Australia (2023). *Australian Cyber Security Strategy 2023-2030*. Department of Home Affairs, Canberra
[23] Commonwealth of Australia (2024) *National Defence Strategy*. Department of Defence, Canberra.

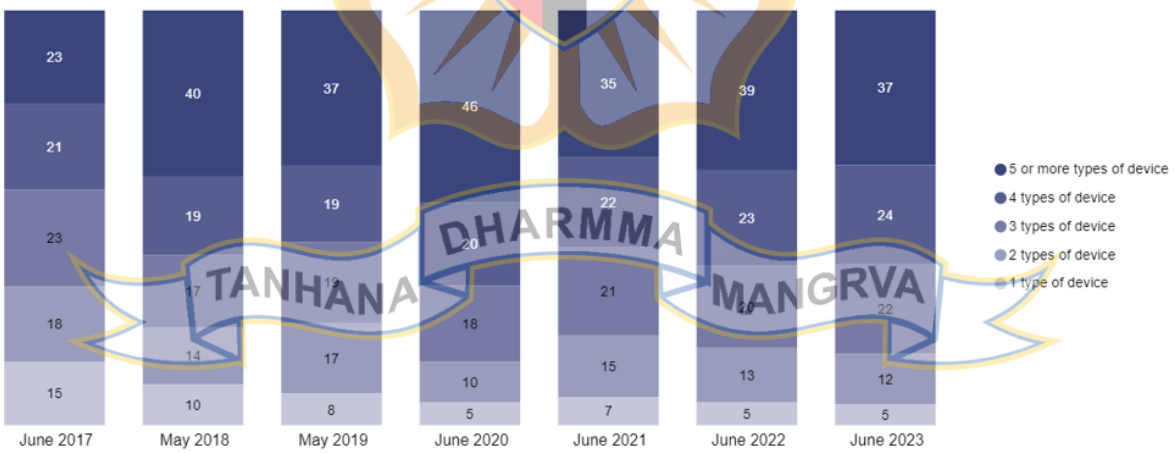
Komunikasi dan Media Australia) pada bulan Juni 2023, 99% orang dewasa yang disurvei telah mengakses internet dalam 6 bulan sebelumnya. Persentase ini tetap stabil sejak meningkat dari 90% pada tahun 2019.[24]



Gambar 1. Persentase Orang Dewasa Australia Online vs Offline

Sumber: *Australian Communication and Media Authority*, 2023.[25]

Rata-rata, orang dewasa Australia menggunakan empat jenis perangkat berbeda untuk mengakses internet dan 37% menggunakan lima perangkat atau lebih untuk mengakses internet. Sebagian besar pengguna internet (89%) mengakses internet dengan ponsel setidaknya sekali sehari dan 86% melakukannya beberapa kali sehari.[26]



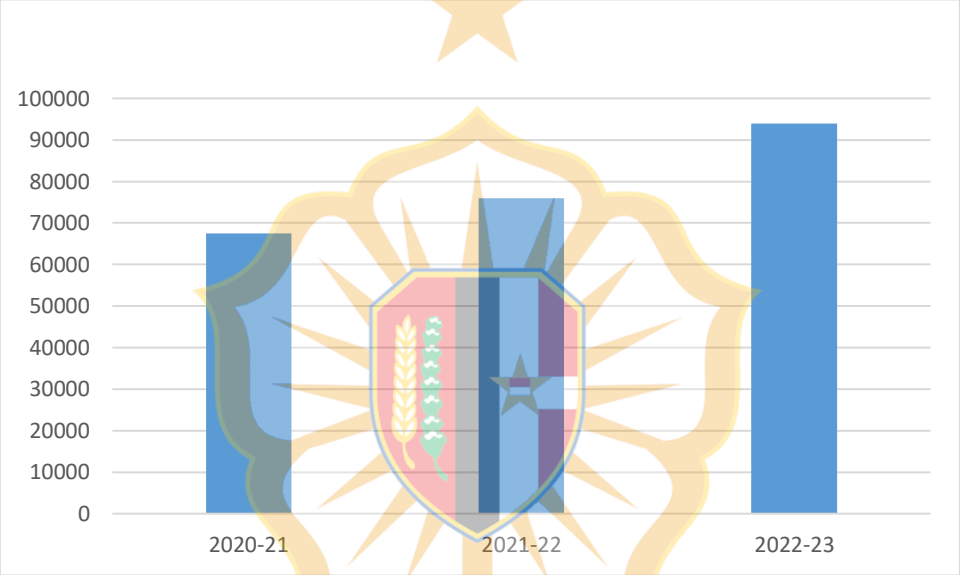
Gambar 2. Jumlah Perangkat Yang Digunakan Untuk Mengakses Internet

Sumber: *Australian Communication and Media Authority*, 2023.[27]

[24] Australian Communications and Media Authority (2023). *Communications and Media in Australia: How We Use the Internet.* https://www.acma.gov.au/publications/2023-12/report/communications-and-media-australia-how-we-use-internet
[25] *Ibid*.
[26] *Ibid.*
[27] *Ibid*.

b. Frekuensi insiden siber dan biaya ekonomi

Jumlah serangan siber yang dilaporkan di Australia terus meningkat dari tahun ke tahun, mencerminkan meningkatnya frekuensi dan kecanggihan ancaman siber. Meningkatnya jumlah serangan juga didorong oleh meluasnya lanskap digital dan menjamurnya perangkat yang saling terhubung, sehingga memberikan lebih banyak peluang untuk aktivitas jahat. *Australian Signals Directorate* (ASD, Direktorat Sinyal Australia) menerima hampir 94.000 laporan insiden siber pada tahun Juli 2022–Juni 2023, naik 23 persen dari tahun sebelumnya. Ini setara dengan rata-rata satu laporan setiap enam menit.[28]

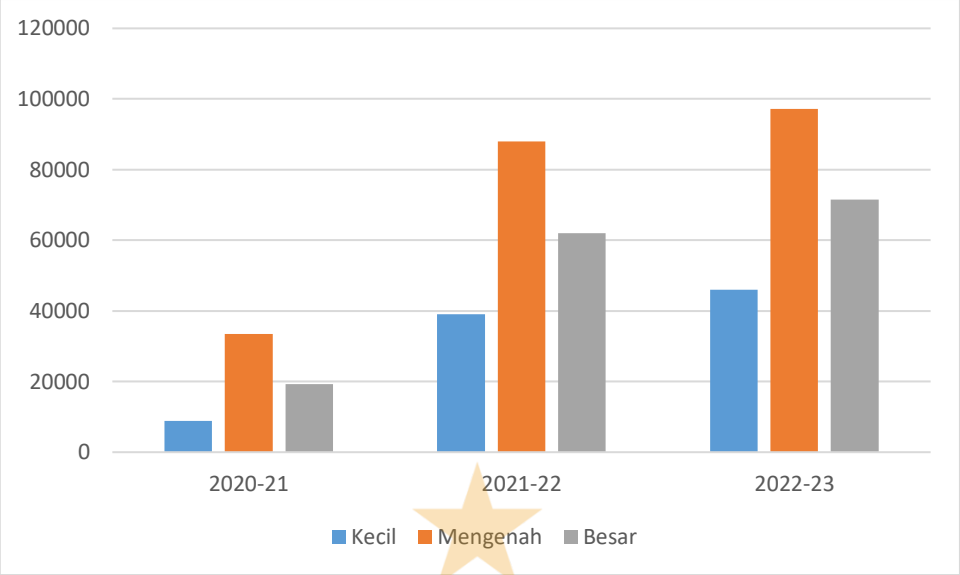


Gambar 3. Jumlah Laporan Insiden Siber ke ASD

Sumber: dibuat oleh penulis mengunakan data dari ASD.[29][30][31]

Kerugian yang ditanggung bisnis Australia akibat insiden siber juga meningkat. Biaya rata-rata insiden siber per laporan ke ASD meningkat 14% dibandingkan tahun sebelumnya.[32]

[28] ASD, *Cyber Security Threat Report 2022-2023*, o*p.cit.*
[29] *Ibid*.
[30] ASD (2022), *ASD Cyber Threat Report 2021-22*. https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf
[31] ASD (2021), *Cyber Security Threat Report 2020-2021*. https://www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Annual%20Cyber%20Threat%20Report%20-%202020-2021.pdf
[32] ASD, Cyber Security Threat Report 2022-2023, o*p.cit.*



Gambar 4. Biaya Rata-rata Insiden Siber Menurut Ukuran Perusahaan

Sumber: dibuat oleh penulis mengunakan data dari ASD.[33][34][35]

c. Jenis insiden siber di Australia

Baik aktor negara maupun non-negara terus menunjukkan niat dan kemampuan untuk menargetkan jaringan Australia baik secara oportunis maupun disengaja. Operasi siber telah menjadi metode pilihan untuk campur tangan dan spionase asing, yang mencerminkan tren global di mana negara-negara menggunakan kemampuan siber untuk mendapatkan keuntungan strategis tanpa terlibat konflik langsung. Aktor-aktor negara terus menargetkan infrastruktur penting di Australia untuk kegiatan pengumpulan informasi atau gangguan.[36] Pada tahun keuangan Juli 2022 – Juni 2023 ASD merespons beberapa pelanggaran data signifikan yang melibatkan eksfiltrasi data dari infrastruktur penting.[37]

Menurut ASD, tiga kejahatan siber yang paling banyak dialami individu adalah penipuan identitas, penipuan perbankan online, dan penipuan belanja online. Sebaliknya, dunia usaha cenderung menjadi korban penyusupan email, penyusupan email bisnis, penipuan, dan penipuan perbankan online.[38] Penjahat siber mengembangkan operasi mereka terhadap organisasi-

[33] *Ibid*.
[34] ASD, Cyber Security Threat Report 2021-2022 *op.cit.*
[35] ASD, Cyber Security Threat Report 2020-2021 *op.cit.*
[36] ASD, Cyber Security Threat Report 2022-2023 *op.cit.*
[37] *Ibid.*
[38] *Ibid*. h.13

organisasi Australia, dengan peningkatan insiden terkait pemerasan selama 18 bulan terakhir. Dari 127 insiden yang direspon ASD pada tahun keuangan 2022-2023, 118 diantaranya melibatkan *ransomware* atau bentuk pembatasan lainnya terhadap file, sistem, atau akun.[39] Meningkatnya prevalensi dan dampak *ransomware* tidak hanya mengganggu operasional tetapi juga menimbulkan kerugian finansial yang signifikan bagi para korban. Meningkatnya serangan penolakan layanan juga menunjukkan pergeseran ke arah metode yang dapat melumpuhkan aktivitas bisnis dan layanan.

Tidak semua ancaman siber merupakan ancaman langsung terhadap keamanan nasional, namun dampak kumulatifnya dapat mengganggu kehidupan sehari-hari dan stabilitas perekonomian secara signifikan. Misalnya, serangan siber yang menargetkan usaha kecil, lembaga pendidikan, atau penyedia layanan kesehatan mungkin tidak langsung membahayakan keamanan nasional, namun dapat menyebabkan kerugian finansial, pelanggaran data, dan gangguan layanan yang berdampak pada perekonomian yang lebih luas. Insiden-insiden ini menggarisbawahi pentingnya memperkuat langkah-langkah keamanan siber secara universal. Dengan memastikan bahwa semua sektor, termasuk sektor yang dianggap kurang penting, terlindungi dengan baik, bisa dibangun infrastruktur siber yang lebih tangguh. Pendekatan holistik ini tidak hanya membantu mencegah eskalasi serangan kecil menjadi ancaman yang lebih besar namun juga menumbuhkan kepercayaan masyarakat terhadap sistem digital, sehingga mendukung keamanan dan stabilitas masyarakat digital secara keseluruhan.

10. Kerangka Teoretis

a. Realisme

Realisme menekankan peran negara-bangsa sebagai aktor utama dalam hubungan internasional. Teori ini berfokus pada kekuasaan dan keamanan dengan alasan bahwa negara pada dasarnya hanya mementingkan diri sendiri dan beroperasi dalam sistem internasional yang anarkis.[40] Realisme berpendapat bahwa sifat anarkis sistem internasional memaksa negara-negara

[39] *Ibid*
[40] Korab-Karpowicz, J. (2023) 'Political Realism in International Relations', *Stanford Encyclopedia of Philosophy.* https://plato.stanford.edu/entries/realism-intl-relations/

untuk memprioritaskan kelangsungan hidup dan kekuasaan, dengan distribusi kekuasaan di antara negara-negara mempengaruhi perilaku mereka.[41] Menurut realisme, tanggung jawab utama negara adalah melindungi warga negaranya dari ancaman eksternal. Negara muncul dari kontrak sosial di mana individu melepaskan kebebasan tertentu sebagai imbalan atas perlindungan negara dan penegakan hukum dan ketertiban.[42]

Realisme, dengan fokusnya pada kekuasaan, keamanan, dan kepentingan pribadi negara, memberikan kerangka kerja penting untuk memahami keamanan siber di era modern. Dilihat dari perspektif realisme, dunia maya merupakan domain bagi negara untuk menegaskan kekuasaan dan melindungi kepentingan nasionalnya. Sifat anarkis dalam sistem internasional, dimana tidak ada otoritas pusat untuk menegakkan peraturan dan norma, tercermin dalam dunia maya yang tidak diatur dan tidak memiliki batas negara. Negara-negara, yang didorong oleh keharusan untuk bertahan hidup, terlibat dalam spionase siber, perang siber, dan pengembangan kemampuan siber yang ofensif dan defensif untuk mempertahankan keunggulan strategis mereka. Pandangan realisme melihat operasi siber sebagai perpanjangan dari strategi militer tradisional, di mana negara memanfaatkan alat siber untuk mencapai tujuan strategis, mengumpulkan intelijen, mengganggu operasi musuh, dan mencegah potensi ancaman.

Realisme menekankan sifat kompetitif dan *zero-sum* dalam hubungan internasional, yang terlihat jelas dalam domain siber. Negara-negara berinvestasi besar-besaran dalam langkah-langkah keamanan siber untuk melindungi infrastruktur penting, aset ekonomi, dan sistem militer dari ancaman siber yang ditimbulkan oleh negara-negara pesaing dan aktor non-negara. Realisme juga menyoroti pentingnya proyeksi kekuatan dan pencegahan di dunia maya. Negara-negara menggunakan kemampuan siber tidak hanya untuk pertahanan tetapi juga untuk menunjukkan kekuatan dan tekad, yang bertujuan untuk mencegah musuh melancarkan serangan siber.

---

[41] Antunes, S. dan Camisao, I. (2018) *Introducing Realism in International Relations Theory*. https://www.e-ir.info/2018/02/27/introducing-realism-in-international-relations-theory/#google_vignette

[42] Williams, M.C. (2009). *The Realist Tradition and the Limits of International Relations*. Cambridge University Press, United Kingdom

Dalam pandangan realisme, negara-negara sangat menyadari perlunya menjaga keseimbangan kekuatan siber untuk mencegah suatu negara memperoleh keuntungan yang tidak proporsional. Dalam konteks ini, pencegahan siber menjadi komponen kunci strategi keamanan nasional. Negara-negara berupaya untuk membangun kemampuan pencegahan yang kredibel dengan menunjukkan kemampuan mereka untuk mengidentifikasi penyerang dan merespons dengan kekuatan yang proporsional atau lebih besar, sehingga menghalangi pihak-pihak yang bermusuhan untuk memulai konflik siber. Perspektif realisme mengakui bahwa aliansi dalam domain siber dapat berguna untuk mengumpulkan sumber daya dan meningkatkan pertahanan kolektif terhadap ancaman bersama. Namun kerja sama ini dipandang sebagai langkah strategis karena dilatarbelakangi oleh kepentingan pribadi. Ini adalah sarana untuk mencapai tujuan dan digunakan untuk mencapai tujuan tertentu atau memajukan keamanan.

b. Neoliberalisme

Neoliberalisme (kadang-kadang disebut institusionalisme liberal) menekankan kerja sama dan saling ketergantungan antar negara-bangsa. Teori ini berargumen bahwa lembaga-lembaga internasional, saling ketergantungan ekonomi, dan pemerintahan demokratis dapat memitigasi sifat anarkis sistem internasional dan mendorong perdamaian dan kerja sama.[43] Tujuan Neoliberalisme adalah untuk memahami bagaimana lembaga-lembaga internasional memelihara dan memperdalam kerja sama internasional. Diasumsikan bahwa pertumbuhan lembaga-lembaga ini merupakan perkembangan yang positif.[44]

Neoliberalisme berpendapat bahwa meskipun sistem internasional bersifat anarkis, negara-negara dapat bekerja sama untuk mengatasi tantangan bersama. Di bidang keamanan siber, hal ini tercermin dalam penetapan norma, perjanjian, dan kerangka kerja sama internasional yang bertujuan untuk meningkatkan stabilitas siber global. Institusi seperti Perserikatan Bangsa-Bangsa dan organisasi regional memainkan peran

[43] Dunne, T, Kurki, M dan Smith, S. (2020) *International Relations Theories: Discipline and Diversity (edisi 5).* Oxford University Press: United Kingdom.
[44] *Ibid*.

penting dalam mendorong dialog, menetapkan standar, dan memfasilitasi kerja sama antar negara untuk memerangi kejahatan siber, melindungi infrastruktur penting, dan meningkatkan ketahanan siber.

Perspektif neoliberal menggarisbawahi pentingnya saling ketergantungan dan manfaat kerja sama di dunia maya. Sifat ekonomi digital global yang saling terhubung berarti bahwa tidak ada negara yang kebal terhadap ancaman siber, sehingga kolaborasi menjadi hal yang penting. Negara, dunia usaha, dan aktor non-negara diberi insentif untuk berbagi informasi, praktik terbaik, dan teknologi guna meningkatkan postur keamanan siber kolektif mereka. Kemitraan pemerintah-swasta sangat penting dalam konteks ini, karena harus memanfaatkan keahlian dan sumber daya dari kedua sektor untuk mengatasi tantangan siber yang kompleks. Upaya kerja sama ini saling menguntungkan, mengurangi risiko insiden siber secara keseluruhan, dan menciptakan lingkungan siber yang lebih aman dan stabil.

Neoliberalisme menyoroti peran transparansi dan upaya membangun kepercayaan dalam mendorong keamanan siber. Langkah-langkah membangun kepercayaan, seperti transparansi dalam kemampuan dan kebijakan siber, latihan siber bersama, dan pembentukan saluran komunikasi, membantu mengurangi kesalahpahaman dan mencegah eskalasi di dunia siber. Dengan mengembangkan pendekatan yang kooperatif dan transparan, negara dapat membangun kepercayaan dan meningkatkan kemampuan kolektif mereka untuk merespons ancaman siber. Neoliberalisme berpendapat bahwa melalui keterlibatan dan kepatuhan yang berkelanjutan terhadap norma dan perjanjian yang telah ditetapkan, komunitas internasional dapat menciptakan lanskap siber yang lebih dapat diprediksi dan aman, yang pada akhirnya akan menguntungkan semua pihak dengan mengurangi kemungkinan konflik dan meningkatkan ketahanan siber global.

c. Teori kontrak sosial

Teori kontrak sosial menyatakan bahwa individu menyetujui, baik secara eksplisit maupun implisit, untuk membentuk masyarakat dan membentuk otoritas pemerintahan dengan imbalan perlindungan dan manfaat tertentu. Teori ini, yang dikemukakan oleh para pemikir seperti Thomas Hobbes, John Locke, dan Jean-Jacques Rousseau, menyatakan bahwa jika tidak ada

kesepakatan seperti itu, individu akan berada dalam "keadaan alami" yang ditandai dengan kekacauan dan ketidakamanan.[45] Kontrak sosial mewakili perjanjian implisit di mana individu menyerahkan sebagian kebebasan mereka dan tunduk pada otoritas negara dengan imbalan keamanan, ketertiban, dan perlindungan hak-hak dasar mereka. Kerangka ini memberikan dasar untuk memahami legitimasi kekuasaan pemerintahan dan kewajiban negara terhadap warganya, dengan menekankan hubungan timbal balik antara hak individu dan pemerintahan kolektif.[46]

Dengan menerapkan teori kontrak sosial pada keamanan siber, dunia digital dapat dilihat sebagai “keadaan alami” modern di mana, tanpa regulasi, individu dan organisasi menghadapi ancaman signifikan seperti serangan siber, pelanggaran data, dan bentuk kejahatan siber lainnya. Dalam konteks ini, peran negara adalah bertindak sebagai otoritas berdaulat yang menegakkan ketertiban dan keamanan di dunia maya. Hal ini melibatkan pengembangan dan penegakan kebijakan, peraturan, dan kerangka keamanan siber yang komprehensif yang melindungi infrastruktur digital dan data warganya. Negara harus membangun mekanisme pertahanan yang kuat, melakukan deteksi ancaman secara proaktif, dan memastikan kemampuan respons yang cepat untuk melawan ancaman siber secara efektif.

Penekanan teori kontrak sosial pada kekuasaan absolut kedaulatan menggarisbawahi pentingnya otoritas negara dalam mengoordinasikan dan menerapkan langkah-langkah keamanan siber. Hal ini tidak hanya mencakup perlindungan infrastruktur penting nasional tetapi juga regulasi praktik sektor swasta untuk memastikan kepatuhan terhadap standar keamanan siber. Individu dan organisasi diharapkan untuk mematuhi peraturan ini dan bekerja sama dengan inisiatif pemerintah di bidang keamanan siber. Dengan melakukan hal ini, negara memenuhi kewajiban kontrak sosialnya untuk memberikan keamanan dan stabilitas di dunia digital, memastikan bahwa warga negara dapat terlibat dalam aktivitas online tanpa rasa takut terus-menerus terhadap ancaman siber.

---

[45] Britannica, *Social Contract*. https://www.britannica.com/topic/social-contract

[46] Burnyeat, G dan Johansson M.S. (2022), ‘An Anthropology of the Social Contract: The Political Power of an Idea’ *Critique of Anthropology.* Vol 42(3)

Teori kontrak sosial menyiratkan bahwa legitimasi kekuasaan kedaulatan dalam keamanan siber bergantung pada kemampuannya untuk melindungi warga negaranya secara efektif. Jika negara gagal memberikan langkah-langkah keamanan siber yang memadai, maka negara berisiko melanggar kontrak sosial, sehingga menyebabkan hilangnya kepercayaan dan otoritas. Kewajiban ini mencakup upaya perlindungan tidak hanya terhadap ancaman siber eksternal dari negara lain atau pelaku jahat, namun juga mengatasi kerentanan internal seperti praktik keamanan siber yang tidak memadai dalam infrastruktur dan bisnis penting. Di era digital, peran negara mencakup adaptasi dan investasi berkelanjutan dalam teknologi keamanan siber, pendidikan, dan kolaborasi internasional untuk tetap terdepan dalam menghadapi ancaman yang terus berkembang. Dengan memastikan lingkungan digital yang aman dan berketahanan, negara menjunjung tinggi kontrak sosialnya, membina masyarakat yang stabil dan aman di mana individu dapat berkembang tanpa rasa takut terhadap ancaman siber.

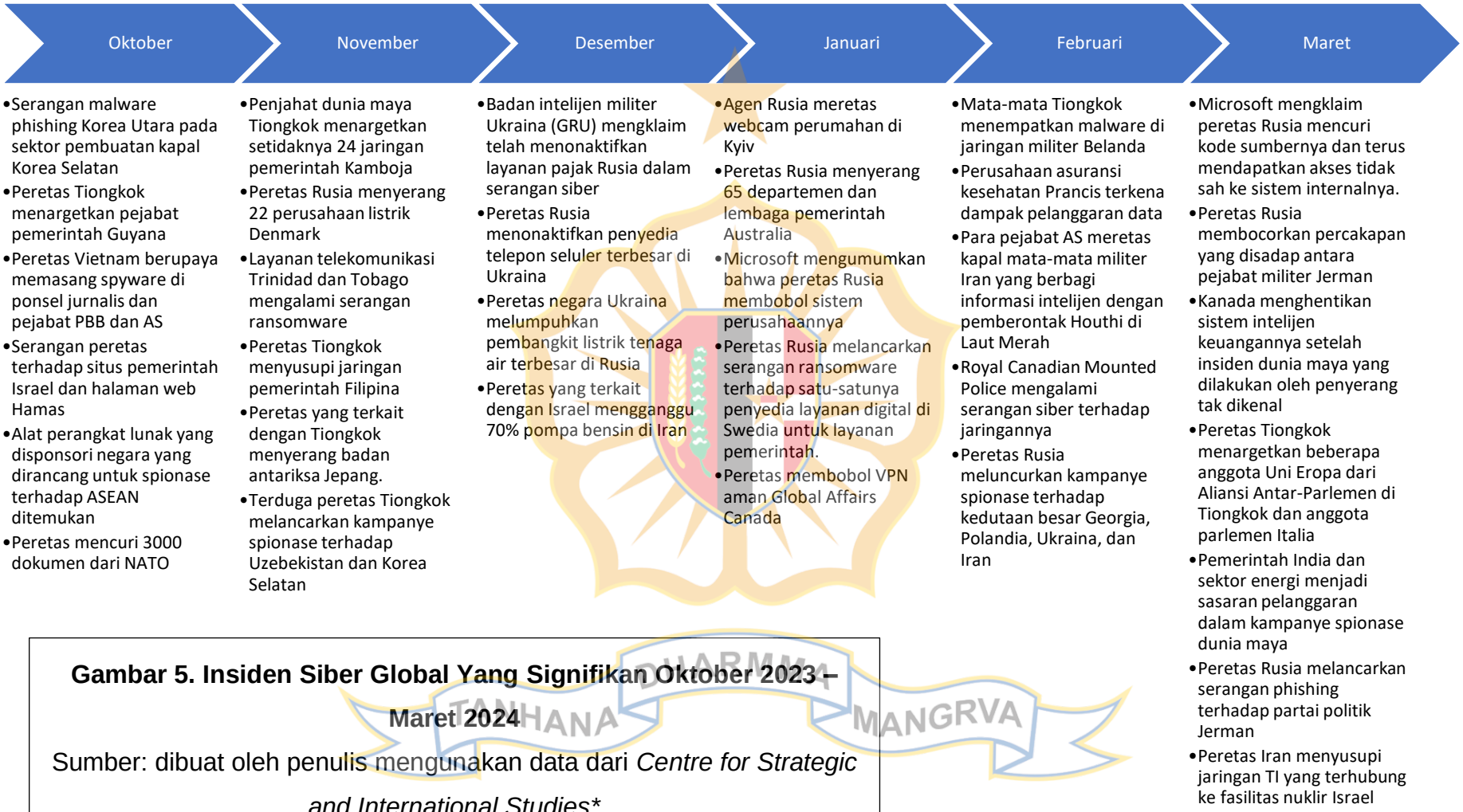
11. Lingkungan Strategis

a. Internasional

Lingkungan strategis internasional saat ini ditandai dengan meningkatnya kompleksitas dan ketidakstabilan, yang didorong oleh munculnya tatanan dunia multipolar. Penyebaran kekuasaan ini telah menciptakan lanskap geopolitik yang kompetitif, dimana aliansi tradisional sedang diuji dan kemitraan baru mulai terbentuk. Saling ketergantungan ekonomi, kemajuan teknologi, dan ancaman transnasional seperti serangan dunia maya, perubahan iklim, dan pandemi menambah kompleksitas hubungan internasional. Selain itu, bangkitnya kembali sentimen nasionalis dan proteksionis, serta terkikisnya lembaga-lembaga multilateral, menantang efektivitas tata kelola global.[47] Dalam kondisi ini, negara-negara berupaya menjaga keseimbangan antara kerja sama dan persaingan, berupaya melindungi kepentingan nasional mereka sambil mengatasi tantangan global yang memerlukan tindakan kolektif.

[47] Lopez-Claros dkk (2020), *Global Governance and the Emergence of Global Institutions for the 21st Century*. Cambridge University Press: United Kingdom.

Tren serangan siber global serupa dengan yang terjadi di Australia – semakin meningkat frekuensi dan signifikansinya. *Centre for Strategic and International Studies* (CSIS) telah mengumpulkan informasi mengenai serangan siber yang dianggap penting bagi keamanan nasional di seluruh dunia. Dari data ini jelas bahwa ancaman siber kini semakin canggih dan terarah, dengan aktor-aktor yang disponsori negara sering kali memimpin serangan-serangan tersebut. Data disediakan di Gambar 5.



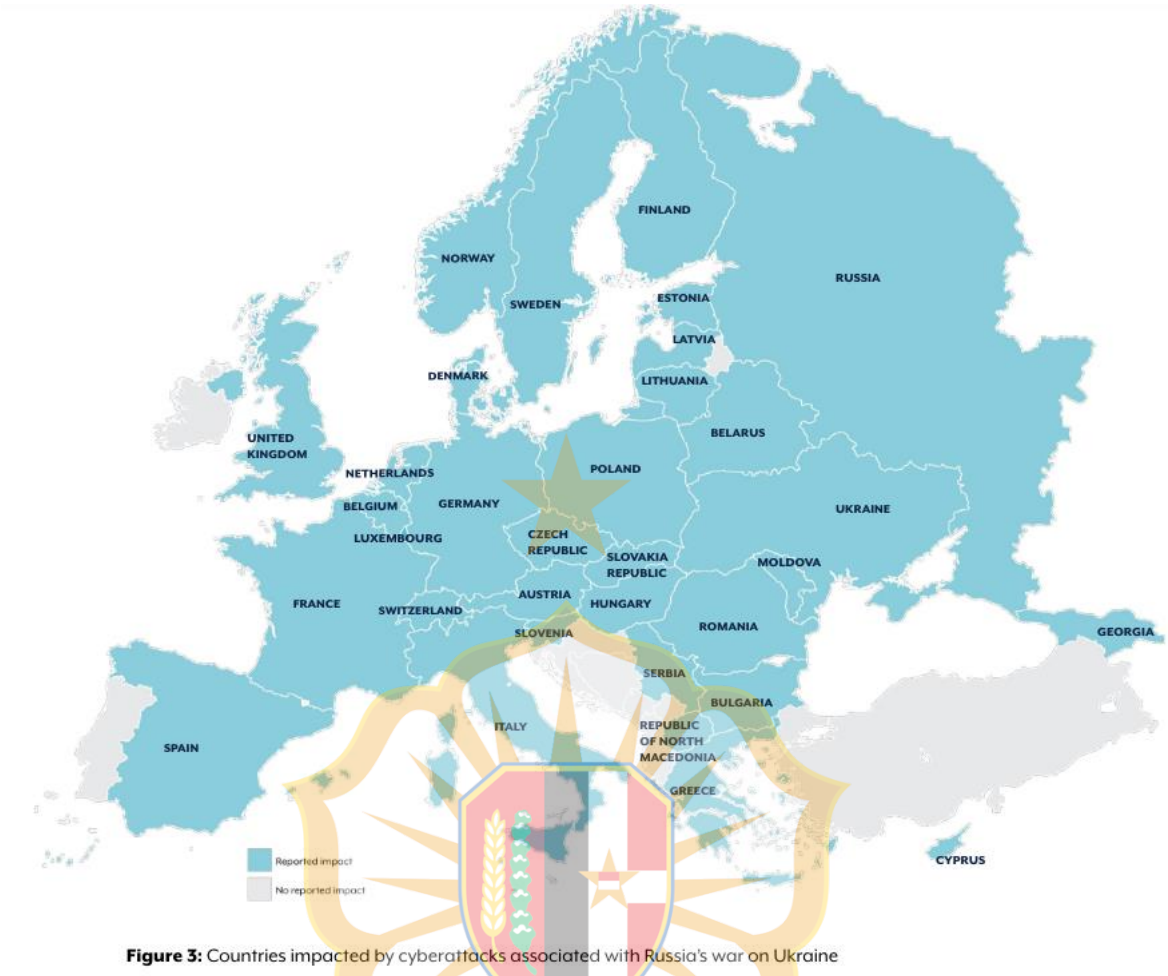
Gambar 5. Insiden Siber Global Yang Signifikan Oktober 2023 – Maret 2024

Sumber: dibuat oleh penulis mengunakan data dari *Centre for Strategic and International Studies**

*CSIS (2024) *Significant Cyber Incidents* https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Negara-negara semakin banyak yang menggunakan operasi siber sebagai pilihan utama untuk membangun keunggulan kompetitif geopolitik mereka, untuk mendukung perekonomian mereka atau mendukung operasi yang menantang kedaulatan negara lain. Perang antara Rusia dan Ukraina ditandai dengan penggunaan operasi siber – yang dilakukan oleh aktor negara dan non-negara – bersamaan dengan aksi militer konvensional. Kedua negara tersebut telah menjadi korban serangan siber yang ditujukan terhadap pemerintah dan jaringan infrastruktur penting.[48] Menurut ASD, pada tahun pertama konflik, *Computer Emergency Response Team*-Eropa (CERT-EU) mengidentifikasi dan menganalisis 806 serangan siber yang terkait dengan konflik tersebut. Hal ini termasuk serangan yang berdampak pada negara-negara lain di Eropa, termasuk Belanda, Jerman dan Inggris.[49]

[48] Mueller, G.B. dkk (2023), *Cyber Operations During the Russo-Ukrainian War.* CSIS https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war
[49] ASD, *Cyber Threat Report 2022-23 op. cit.*



Gambar 6. Negara-negara Eropa Terkena Dampak Serangan Siber Yang Terkait Dengan Perang Rusia-Ukraina

Sumber: ASD Cyber Threat Report 2022-23[50]

Saling ketergantungan ekonomi global dan perkembangan teknologi digital juga memainkan peran penting dalam membentuk lingkungan keamanan siber internasional. Ketika perekonomian menjadi lebih saling terhubung dan bergantung pada infrastruktur digital, potensi dampak serangan siber meningkat. Kerentanan rantai pasokan telah menjadi kekhawatiran yang signifikan, karena insiden siber yang memengaruhi salah satu bagian rantai pasokan global dapat berdampak besar pada bisnis dan perekonomian di seluruh dunia.[51] Selain itu, kebangkitan teknologi seperti

[50] ASD, *Cyber Threat Report 2022-23, op.cit.*
[51] NIST (2022), *NIST Updates Cybersecurity Guidance for Supply Chain Risk Management.* https://www.nist.gov/news-events/news/2022/05/nist-updates-cybersecurity-guidance-supply-chain-risk-management

Internet of Things (IoT), AI, dan jaringan 5G menimbulkan tantangan dan kerentanan keamanan baru. Perselisihan geopolitik mengenai standar teknologi dan kendali atas teknologi-teknologi utama semakin memperumit lanskap keamanan siber.[52] Misalnya, perdebatan mengenai penggunaan peralatan 5G buatan Tiongkok di negara-negara Barat menyoroti titik temu antara keamanan siber dan pertimbangan geopolitik, di mana negara-negara mempertimbangkan risiko spionase dan sabotase dibandingkan dengan manfaat ekonomi dan teknologi.

b. Regional

Lingkungan keamanan siber di kawasan Asia-Pasifik dicirikan oleh lanskap ancaman yang berkembang pesat, didorong oleh pertumbuhan ekonomi yang signifikan di kawasan ini, peningkatan digitalisasi, dan ketegangan geopolitik. Negara-negara di Asia-Pasifik sedang mengalami lonjakan serangan siber, mulai dari *ransomware* dan *phishing* hingga serangan canggih yang disponsori negara yang menargetkan infrastruktur penting dan data sensitif.[53] Misalnya, Jepang dan Korea Selatan telah menghadapi banyak intrusi siber yang dikaitkan dengan aktor-aktor negara yang berupaya mengumpulkan intelijen atau mengganggu layanan.[54] Pertumbuhan ekonomi digital di kawasan ini dan penggunaan teknologi yang luas di berbagai sektor menjadikannya target yang menarik bagi penjahat siber dan aktor-aktor negara.

Menanggapi ancaman yang semakin besar ini, banyak negara di Asia-Pasifik sudah memperkuat kerangka keamanan siber mereka dan berinvestasi pada teknologi keamanan canggih. Jepang, misalnya, telah memperbarui Strategi Keamanan Siber Nasionalnya untuk mengatasi

[52] Neaher dkk (2021), *Standardizing the Future: How Can the United States Navigate the Geopolitics of International Technology Standards?* https://www.atlanticcouncil.org/in-depth-research-reports/report/standardizing-the-future-how-can-the-united-states-navigate-the-geopolitics-of-international-technology-standards/

[53] World Economic Forum (2023). *Why is the Asia Pacific Region A Target for Cybercrime – and What Can be Done About it?* https://www.weforum.org/agenda/2023/06/asia-pacific-region-the-new-ground-zero-cybercrime/

[54] Al Jazeera (2023). *US, Japan, South Korea Step Up Efforts to Counter North Korea Cyber-Threats*. https://www.aljazeera.com/news/2023/12/9/us-japan-south-korea-launch-new-efforts-to-counter-n-korea-cyber-threats

ancaman yang muncul dan meningkatkan kolaborasi dengan mitra internasional. Demikian pula, Singapura telah menerapkan langkah-langkah keamanan siber yang kuat melalui Undang-Undang Keamanan Siber dan membentuk Badan Keamanan Siber untuk mengawasi upaya nasional.[55] Inisiatif-inisiatif ini mencerminkan tren regional menuju pengawasan peraturan yang lebih besar, peningkatan kemitraan publik-swasta, dan peningkatan kerja sama internasional untuk memitigasi risiko siber.

Terlepas dari upaya-upaya ini, masih terdapat tantangan dalam mencapai postur keamanan siber yang kohesif dan efektif di Asia-Pasifik. Keberagaman lingkungan hukum dan peraturan, tingkat kemajuan teknologi yang berbeda-beda, dan perbedaan prioritas strategis dapat menghambat kerja sama regional.[56] Selain itu, pesatnya perubahan teknologi dan canggihnya ancaman siber memerlukan adaptasi dan inovasi berkelanjutan dalam praktik keamanan siber. Untuk mengatasi tantangan ini, organisasi regional seperti ASEAN dan APEC memainkan peran penting dalam mendorong dialog, berbagi praktik terbaik, dan mengoordinasikan inisiatif keamanan siber bersama.[57]

Di wilayah Pasifik, negara-negara sering menjadi sasaran para penjahat siber dan aktor-aktor yang disponsori negara yang bertujuan untuk mengeksploitasi kerentanan dalam infrastruktur penting dan sistem pemerintahan. Misalnya, Vanuatu mengalami serangan siber yang signifikan pada bulan November 2022 ketika serangan *ransomware* sangat mengganggu operasi pemerintah Vanuatu, sehingga memengaruhi layanan darurat, email, dan saluran telepon. Infrastruktur digital pemerintah terkena dampak yang sangat parah, dengan banyak sistem komputer milik pemerintah yang tidak dapat diakses, sehingga menyebabkan banyak keterlambatan dalam pelayanan publik.[58] Menanggapi ancaman yang

[55] Government of Singapore (2021). *The Singapore Cybersecurity Strategy 2021*. Security Agency of Singapore, Singapore.
[56] Tay, K.L. (2023) *ASEAN Cyber-security Cooperation: Towards a Regional Emergency-response Framework*. The International Institute for Strategic Studies: United Kingdom.
[57] *Ibid.*
[58] Mao, F. (2023), *Vanuatu: Hackers Strand Pacific Island Government for Over a Week.* BBC News, 18 November https://www.bbc.com/news/world-asia-63632129

muncul ini, negara-negara Kepulauan Pasifik telah mulai mengembangkan dan menerapkan strategi keamanan siber nasional untuk meningkatkan pertahanan siber dan membangun ketahanan. Kerja sama regional dan dukungan dari mitra internasional memainkan peran penting dalam memperkuat kemampuan keamanan siber di seluruh Pasifik, memberikan bantuan teknis, program peningkatan kapasitas, dan berbagi praktik terbaik untuk mengatasi lanskap ancaman siber yang terus berkembang.[59]

c. Nasional

Pemerintah Australia saat ini, yang terpilih pada tahun 2022, telah mengambil sejumlah langkah untuk memperkuat tata kelola keamanan siber di tingkat nasional. Keamanan siber mendapat portofolio tersendiri di kabinet pemerintah Australia untuk pertama kalinya pada tahun 2022, dengan penunjukan Clare O'Neil sebagai Menteri Dalam Negeri dan Menteri Keamanan Siber. Pada tahun 2023, Pemerintah membentuk Koordinator Siber Nasional untuk mendukung Menteri Keamanan Siber dalam memimpin koordinasi kebijakan keamanan siber nasional, respons terhadap insiden siber besar, upaya kesiapsiagaan insiden siber seluruh pemerintah, dan memperkuat kemampuan keamanan siber Australia.[60]

Pemerintah Australia melakukan investasi besar dalam keamanan siber sebagai bagian dari anggaran federal tahun 2023-2024. Hal ini termasuk alokasi sebesar $101,6 juta dolar Australia selama lima tahun untuk meningkatkan ketahanan siber di sektor swasta dan publik.[61] Pendanaan ini bertujuan untuk memperkuat pertahanan siber negara melalui berbagai inisiatif, termasuk pembentukan Koordinator Siber dengan alokasi

[59] Parliament of Australia (2021). *Australian Government Expenditure*. https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/BudgetReview202021/AustralianGovernmentExpenditure

[60] Prime Minister and Minister for Home Affairs (2023). *Jumpa pers 23 Juni: Appointment of National Cyber Security Coordinator*. https://www.pm.gov.au/media/appointment-national-cyber-security-coordinator

[61] Commonwealth of Australia (2024), *Budget Papers 2023-24.* https://archive.budget.gov.au/2023-24/index.htm

anggaran sebesar $46,5 juta selama empat tahun.[62] Investasi lebih lanjut mencakup $19,5 juta untuk meningkatkan keamanan infrastruktur penting dan membantu merespons serangan siber yang signifikan, dan $23,4 juta untuk program sipir siber usaha kecil yang bertujuan membangun kemampuan siber internal dalam usaha kecil dan menengah.[63] Selain itu, pemerintah juga mendedikasikan $88,8 juta selama dua tahun untuk mendukung Hak Data Konsumen, yang mencakup peningkatan keamanan siber untuk memastikan pembagian data online yang lebih aman bagi konsumen.[64]

Pendanaan yang diuraikan di atas merupakan tambahan dari pendanaan untuk REDSPICE (*Resilience, Effects, Defence, Space, Intelligence, Cyber, Enablers*; Ketahanan, Efek, Pertahanan, Luar Angkasa, Intelijen, Siber, Pemberdaya), sebuah inisiatif keamanan siber dan intelijen yang dirancang untuk meningkatkan kemampuan ASD. Diluncurkan pada tahun 2022 dengan komitmen sebesar $9,9 miliar selama dekade hingga tahun 2032, REDSPICE bertujuan untuk melipatgandakan kemampuan perang siber ASD dan menggandakan kemampuannya dalam mendeteksi dan merespons ancaman siber. Investasi ini akan mendukung operasi intelijen, teknologi dasar, ketahanan dan redundansi.[65]

12. Peluang dan Kendala

Lingkungan strategis nasional, regional dan internasional menimbulkan peluang dan kendala pada optimalisasi infrastruktur siber Australia. Hal ini terlihat dari beberapa aspek, antara lain aspek demografi, geografi, ideologi, politik, sosial budaya, ekonomi dan pertahanan keamanan.

---

[62] Australian Information Security Association (2024), *Australian Federal Government's 2024-25 Budget.* https://www.aisa.org.au/Public/Public/News_and_Media/News/2024/Australian-Federal-Government-s-2024-25-Budget.aspx
[63] *Ibid.*
[64] Commonwealth of Australia, *Budget Papers 2023-24 Op.Cit.*
[65] Australian Signal's Directorate (2022), *REDSPICE: A Blueprint for Growing ASD's Capabilities.* https://www.asd.gov.au/sites/default/files/2022-05/ASD-REDSPICE-Blueprint.pdf

a. Demografi

1) Peluang: Penetrasi internet yang tinggi di Australia, dengan 99% orang dewasa mengakses internet, memberikan landasan yang kuat bagi inisiatif digital. Populasi yang paham teknologi dapat dimanfaatkan untuk meningkatkan kesadaran dan keterampilan keamanan siber. Memanfaatkan masyarakat Australia yang beragam secara demografis akan menghasilkan beragam keterampilan dan perspektif terhadap masalah keamanan siber.
2) Kendala: Meningkatnya penggunaan internet oleh penduduk Australia di berbagai perangkat dapat menciptakan lebih banyak titik kerentanan untuk diserang.

b. Geografi

1) Peluang: Kemitraan regional di Asia-Pasifik dapat meningkatkan langkah-langkah keamanan siber kolektif
2) Kendala: Luasnya geografis Australia dan banyaknya wilayah terpencil mungkin menimbulkan tantangan dalam menerapkan langkah-langkah keamanan siber yang seragam. Isolasi geografis tidak memberikan perlindungan yang sama terhadap serangan siber seperti terhadap serangan militer konvensional.

c. Ideologi

1) Peluang: Komunikasi yang dilakukan pemerintah mengenai pentingnya keamanan dan ketahanan dapat menciptakan visi kolektif untuk mendorong kebijakan keamanan siber yang kuat. Komitmen terhadap nilai-nilai demokrasi dan privasi dapat menumbuhkan kepercayaan dan kerja sama dalam inisiatif keamanan siber.
2) Kendala: Menyeimbangkan privasi dan keamanan dapat menimbulkan tantangan peraturan dan potensi penolakan dari masyarakat. Perbedaan ideologi dengan mitra internasional dapat menghambat kohesifnya strategi keamanan global.

d. Politik

1) Peluang: Prioritas pemerintah terhadap keamanan siber, seperti terlihat dalam pembentukan portfolio khusus dan alokasi anggaran, memberikan peluang untuk mempercepat pembangunan infrastruktur siber yang matang.
2) Kendala: Perubahan dan pergeseran politik dapat menyebabkan kebijakan dan pendanaan keamanan siber tidak konsisten. Proses birokrasi dapat memperlambat penerapan langkah-langkah keamanan siber yang penting.

e. Sosial Budaya

1) Peluang: Tingkat literasi digital dan kesadaran masyarakat yang tinggi dapat meningkatkan upaya keamanan siber berbasis masyarakat. Menempatkan penekanan budaya pada inovasi dan teknologi dapat mendorong kemajuan dalam solusi keamanan siber.
2) Kendala: Lanskap sosio-kultural Australia yang beragam mungkin memerlukan pendekatan yang disesuaikan dengan pendidikan dan kebijakan keamanan siber. Mungkin terdapat penolakan sosio-kultural terhadap perubahan peraturan privasi dan keamanan data.

f. Ekonomi

1) Peluang: Perekonomian Australia yang relatif kuat memungkinkan adanya investasi besar dalam infrastruktur dan inovasi keamanan siber. Insentif ekonomi dapat digunakan untuk mendorong kepatuhan luas terhadap langkah-langkah keamanan siber.
2) Kendala: Tingginya dampak ekonomi akibat insiden siber, yang meningkat setiap tahunnya, merupakan tantangan yang signifikan. Usaha kecil dan menengah mungkin harus menghadapi beban keuangan dalam menerapkan langkah-langkah keamanan siber yang komprehensif. Meningkatnya

biaya asuransi siber dan denda peraturan atas pelanggaran menambah tekanan ekonomi pada dunia usaha.

g. Pertahanan Keamanan

1) Peluang: Menekankan pentingnya keamanan siber bagi keamanan nasional dapat mendorong kepatuhan terhadap peraturan dan langkah-langkah keamanan lainnya. Investasi pada kemampuan pertahanan siber dan operasi intelijen dapat meningkatkan ketahanan siber Australia. Potensi peningkatan kolaborasi dengan sekutu internasional untuk meningkatkan pertahanan keamanan siber kolektif.
2) Kendala: Ancaman siber semakin canggih baik dari pihak negara maupun non-negara. Ada kebutuhan yang berkelanjutan untuk adaptasi dan investasi untuk mengimbangi ancaman siber yang berkembang pesat. Terdapat potensi kerentanan dalam rantai pasokan Australia dan ketergantungan pada penyedia teknologi global.

BAB III
PEMBAHASAN

13. Umum

Bab ini akan menyajikan hasil analisis berdasarkan teori dan lingkungan strategis yang dibahas dalam Bab II untuk mengungkap faktor-faktor yang mempengaruhi kesenjangan antara infrastruktur siber Australia saat ini dan apa yang dianggap optimal untuk melindungi keamanan nasional sehingga dapat dirumuskan solusinya. Pembahasan dalam bab ini meliputi 4 aspek dalam rumusan masalah. Pertama, bab ini akan menganalisis pentingnya membangun infrastruktur siber yang mendukung keamanan nasional. Hal ini mencakup diskusi tentang hubungan antara keamanan siber dan keamanan nasional, dan bagaimana Pemerintah Australia membahas ancaman siber dengan masyarakat. Kedua, dilakukan analisis pengaruh regulasi terhadap infrastruktur siber. Hal ini akan mencakup baik undang-undang maupun standar dan peraturan sukarela. Ketiga dikaji dampaknya infrastruktur siber terhadap keamanan nasional. Diskusi ini akan mencakup analisis kebijakan dan strategi pemerintah yang ada, struktur tata kelola siber Australia, tenaga kerja siber dan aspek teknis infrastruktur siber. Terakhir, bab ini akan menyajikan strategi optimalisasi infrastruktur siber. Setelah menganalisis pentingnya kolaborasi domestik dan internasional, Taskap ini akan menguraikan rencana aksi strategis yang spesifik, terukur, dapat dicapai, relevan, dan terikat waktu yang, jika diterapkan, akan mengoptimalkan infrastruktur siber Australia dan melindungi keamanan nasional.

14. Pentingnya Membangun Infrastruktur Siber Yang Mendukung Keamanan Nasional

a. Hubungan antara keamanan siber dan keamanan nasional

Pembahasan mengenai hubungan siber dan keamanan nasional harus terlebih dahulu memahami arti kata 'keamanan'. Teori politik tradisional biasanya memusatkan gagasan keamanan pada negara. Dalam perspektif realisme, negara adalah satu-satunya objek rujukan keamanan, dengan penekanan diberikan pada integritas wilayah dan perlindungan militer. Aliran

pemikiran kedua memperluas gagasan tradisional tentang keamanan hingga mencakup individu. Konsep *human security* (keamanan manusia) pertama kali diperkenalkan pada *Human Development Report* (Laporan Pembangunan Manusia) tahun 1994 oleh Program Pembangunan PBB. Pemahaman keamanan yang lebih komprehensif ini mencakup tujuh bidang utama keamanan: ekonomi; makanan; kesehatan; lingkungan hidup; pribadi; masyarakat; dan keamanan politik.[66] Ada argumentasi bahwa dengan kemajuan teknologi dan ancaman non-tradisional saat ini, keamanan harus dilihat dari dua perspektif – keamanan negara, serta keamanan individu (atau komunitas). Keamanan negara tidak bisa lagi menjadi satu-satunya pertimbangan. Oleh karena itu, keamanan nasional dalam Taskap ini berarti keamanan negara, perekonomian, masyarakat dan sumber daya, serta tata kelola yang baik dan ketahanan institusi.

Setelah ditetapkan bahwa keamanan nasional didefinisikan dalam Taskap ini secara luas, maka pokok bahasan selanjutnya adalah hubungan antara keamanan nasional dan siber. Aktivitas siber yang berbahaya berpotensi berdampak pada keamanan nasional dalam beberapa cara. Dari sudut pandang negara, meningkatnya ketegangan geopolitik di antara negara-negara besar semakin terwujud dalam bentuk spionase siber, serangan siber, dan bentuk agresi siber lainnya yang bertujuan untuk mendapatkan keuntungan strategis. Kelompok pelaku siber yang disponsori negara, sering dikaitkan dengan badan intelijen dan militer, melakukan operasi untuk mencuri informasi sensitif, mengganggu infrastruktur penting, dan merusak stabilitas negara-negara pesaing. Meskipun serangan siber terhadap kepentingan pemerintah Australia tidak selalu diatribusikan secara publik, Direktur Jenderal ASD, Rachel Noble, mengidentifikasi pada tahun 2021 bahwa “aktor negara melakukan pengumpulan intelijen, pengintaian, dan melakukan pra-posisi perangkat lunak berbahaya” di Australia untuk mendapatkan keuntungan strategis.[67] Pada bulan November 2023, Menteri Dalam Negeri dan Keamanan

[66] PBB (1994), *Human Development Report 1994*. Oxford University Press: New York
[67] Noble, R (2021), *ASD: 75 Years and Ready for Tomorrow* (pidato, National Press Club, 18 November). https://www.asd.gov.au/news-events-speeches/speeches/director-general-asd-speech-national-press-club

Siber, Clare O'Neil, mengidentifikasi bahwa Tiongkok, Rusia, dan Iran terlibat dalam serangan siber terhadap kepentingan Australia.[68]

Ketika semakin banyak negara mengembangkan kemampuan siber yang canggih, risiko konflik siber pun meningkat. Meningkatnya kemampuan siber juga meningkatkan risiko alat dan teknik siber jatuh ke tangan aktor non-negara, termasuk kelompok teroris dan organisasi kriminal, sehingga semakin memperumit lanskap keamanan siber. Pemerintah Australia telah secara terbuka menyatakan bahwa geng *ransomware* Rusia yang bernama *REvil* bertanggung jawab atas serangan *ransomware* pada tahun 2022 terhadap perusahaan asuransi kesehatan Medibank, yang berdampak pada hampir 10 juta warga Australia.[69] Serangan yang dilakukan oleh entitas non-negara ini berdampak pada keamanan negara dan manusia di Australia. Kompromi besar-besaran terhadap data pribadi berdampak pada keamanan psikologis sebagian besar penduduk dan mengikis kepercayaan publik terhadap kemampuan lembaga swasta dan pemerintah untuk melindungi keamanan pribadi mereka.

Infrastruktur penting di Australia – termasuk listrik, perbankan, telekomunikasi dan layanan kesehatan – dimiliki oleh lembaga swasta dan publik. Sektor ini sangat penting bagi tujuh aspek keamanan manusia, dan merupakan hal mendasar bagi keselamatan dan kesejahteraan Australia secara keseluruhan. Akibatnya, tindakan siber apa pun yang membahayakan penyediaan layanan penting bisa menjadi potensi ancaman keamanan nasional. Ancaman ini semakin besar karena pertahanan nasional Australia (dari sudut pandang militer) sangat bergantung pada layanan ini. Infrastruktur penting menyediakan layanan penting – termasuk jaringan listrik dan komunikasi – yang memungkinkan ADF berfungsi secara efektif dan merespons ancaman. Namun, infrastruktur penting Australia menjadi sasaran serangan siber yang jumlahnya semakin meningkat. ASD menanggapi 143

[68] O'Neil (2023), *Jumpa Pers 22 November.* https://minister.homeaffairs.gov.au/ClareONeil/Pages/Press-conference-22112023.aspx
[69] Fell, J (2024), 'Medibank Hacker Linked to Russian Hacking Syndicat REvil', *ABC News* https://www.abc.net.au/news/2024-01-24/medibank-hacker-linked-to-russian-hacking-syndicate-revil/103381342

insiden siber yang dilaporkan oleh entitas infrastruktur penting pada periode Juni 2022 – Juli 2023, meningkat dari 95 insiden pada tahun sebelumnya.[70]

Meski tidak dapat dipungkiri bahwa serangan siber berpotensi mengancam keamanan nasional, namun perlu diingat bahwa tidak semua ancaman keamanan siber mengancam keamanan nasional secara langsung. Kejahatan siber tingkat rendah, seperti insiden kecil *ransomware* dan pelanggaran data lokal dapat menyebabkan kerugian besar bagi individu dan bisnis, namun tidak memiliki implikasi keamanan nasional yang signifikan. Demikian pula, serangan terhadap layanan yang tidak vital, meskipun mengganggu dan memakan biaya besar, biasanya tidak menimbulkan ancaman langsung terhadap keamanan nasional. Namun demikian, pola serangan yang sering terjadi di berbagai sektor bisnis dapat mengikis kepercayaan terhadap langkah-langkah keamanan siber nasional dan berkontribusi pada kerentanan keamanan yang lebih luas. Perekonomian modern sangat bergantung pada teknologi dan platform digital, yang menjadikan keamanan siber sebagai landasan ketahanan perekonomian. Serangan siber dapat menyebabkan kerugian finansial yang signifikan, mengganggu operasional bisnis, dan melemahkan kepercayaan konsumen. Kepercayaan masyarakat dan keyakinan terhadap kemampuan pemerintah untuk melindungi warga negaranya merupakan hal mendasar bagi masyarakat yang stabil dan berfungsi.

Jelas dari analisis di atas bahwa keamanan siber tidak bisa lagi dipandang dan didekati sebagai persoalan teknis sederhana; isu ini telah berkembang menjadi tantangan yang beragam dan kompleks yang mencakup dimensi ekonomi, sosial, politik, dan strategis. Meningkatnya frekuensi dan kecanggihan serangan siber mempunyai potensi implikasi keamanan yang lebih dari sekedar gangguan teknis sederhana. Saat ini, pelanggaran keamanan siber dapat merusak kepercayaan publik terhadap institusi, membahayakan informasi keamanan pribadi dan nasional yang sensitif, mengganggu infrastruktur penting, dan bahkan mempengaruhi proses demokrasi dan politik. Oleh karena itu, manajemen keamanan siber yang efektif memerlukan pendekatan holistik yang mengintegrasikan strategi hukum,

[70] ASD, *Cyber Threat Report 2022-23, op.cit.*

kebijakan, sumber daya, dan tata kelola. Hal ini membutuhkan kerja sama antar pemerintah dan industri, komunitas ilmiah dan akademis, serta dengan masyarakat.

b. Diskusi publik tentang siber sebagai ancaman keamanan nasional

Kekhawatiran terhadap ketahanan siber Australia pertama kali dibahas dalam dokumen kebijakan publik pemerintah dalam **Buku Putih Pertahanan tahun 2000**, yang menyatakan bahwa "Australia menghadapi banyak permasalahan keamanan selain yang melibatkan kekuatan militer. Hal ini termasuk potensi ancaman non-militer, seperti serangan siber."[71] Buku Putih tahun 2000 juga mencatat bahwa pemerintah akan mengembangkan "pendekatan nasional yang komprehensif" terhadap tantangan serangan siber terhadap infrastruktur informasi penting Australia.[72] **Buku Putih Pertahanan tahun 2009** menyebutkan siber sebanyak 32 kali, naik dari tiga kali dalam Buku Putih sebelumnya. Dokumen tersebut menyatakan bahwa dalam sepuluh tahun terakhir, operasi di dunia maya menjadi semakin penting, dan "keamanan nasional berpotensi terganggu oleh serangan siber terhadap pertahanan kita, jaringan informasi pemerintah, komersial, atau infrastruktur yang lebih luas."[73]

Strategi keamanan siber pertama Australia, yang dikeluarkan pada tahun 2009, menetapkan kembali ancaman siber sebagai isu prioritas keamanan nasional. Strategi tersebut menetapkan prioritas strategis Pemerintah untuk mengamankan infrastruktur informasi nasional Australia dan mendirikan *Cyber Security Operations Centre* (CSOC), yang kemudian menjadi ACSC.[74] **Strategi keamanan siber yang kedua** pada tahun 2016 membentuk Penasihat Khusus Perdana Menteri bidang Keamanan Siber (yang kini sudah dihentikan). Fokus strategi tahun 2016 adalah pada pertumbuhan, inovasi dan peluang ekonomi, sedangkan aspek keamanan nasional dari siber kurang mendapat perhatian dibandingkan strategi tahun 2009. Meskipun demikian,

---

[71] Commonwealth of Australia (2000), *Defence White Paper 2000,* Department of Defence: Canberra. h.12 p.2.13
[72] *Ibid.* h.13 p.2.19
[73] Commonwealth of Australia, *Defence White Paper 2009,* Department of Defence: Canberra. h.83 p. 9.85
[74] Brangwin, N. (2013). *Cyber Security,* Parliament of Australia. https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/pubs/BriefingBook44p/Cyber#:~:text=In%20November%202009%2C%20the%20Cyber,CERT%20Australia)%20and%20the%%2020CSOC

strategi tahun 2016 secara terbuka mengakui untuk pertama kalinya bahwa Australia memiliki kemampuan siber ofensif yang 'cukup besar'.[75]

Defence Strategic Update (DSU, Pembaruan Strategis Pertahanan) tahun 2020 mencatat bahwa kesediaan sejumlah aktor negara dan non-negara untuk menggunakan kemampuan siber secara jahat memperumit lingkungan strategis Australia.[76] DSU adalah kebijakan pemerintah publik pertama yang menghubungkan aktivitas siber dan disinformasi dengan campur tangan asing dalam perekonomian, sistem politik dan sosial serta infrastruktur. **Strategi keamanan siber ketiga** dirilis pada tahun yang sama. Strategi tersebut mencatat bahwa peran Pemerintah adalah untuk "berfokus pada ancaman-ancaman kritis dan aktor-aktor paling canggih, sambil memastikan dasar ketahanan siber di seluruh perekonomian."[77] Strategi ini menegaskan bahwa tindakan siber yang dilakukan oleh negara-negara dan aktor-aktor yang disponsori negara dapat berdampak pada kepentingan nasional dan keamanan nasional Australia. **Strategi Keamanan Siber Pemerintah yang terbaru** mengacu pada keamanan nasional sebanyak tujuh kali. Laporan ini mencatat bahwa serangan siber dapat menimbulkan kerugian terhadap perekonomian dan keamanan nasional Australia, dan sifat dunia siber yang tidak memiliki batas berarti bahwa kompromi dapat terjadi dari jarak jauh dan dalam skala besar.[78] Saat meluncurkan strategi ini, Menteri Keamanan Siber Clare O'Neil mengatakan bahwa siber "adalah ancaman keamanan nasional yang paling cepat berkembang yang kita hadapi."[79]

Mayoritas warga Australia setuju bahwa serangan siber merupakan ancaman serius terhadap keamanan nasional. *Lowy Institute* tahun 2023 melaporkan bahwa 'serangan siber dari negara lain' merupakan masalah keamanan utama bagi masyarakat Australia, dengan 68 persen responden mengidentifikasinya sebagai 'ancaman kritis' bagi Australia pada dekade

---

[75] Feakin, T. dkk (2016), *Agenda for Change 2016: Cybersecurity*. *Australian Strategic Policy Institute*. https://www.aspistrategist.org.au/agenda-change-cybersecurity/

[76] Commonwealth of Australia, *Defence Strategic Update*, Department of Defence: Canberra h.13 p.1.10

[77] Commonwealth of Australia, *Australia's Cyber Security Strategy 2020,* Department of Home Affairs: Canberra h.20 p.27

[78] Commonwealth of Australia, *Australian Cyber Security Strategy 2023-2030, op.cit.* h.20

[79] O'Neil (2023), *Joint Press Conference with the Assistant Minister for Foreign Affairs*. https://ministers.dfat.gov.au/minister/tim-watts/transcript/joint-press-conference-minister-home-affairs-and-cyber-security

berikutnya.[80] Kekhawatiran ini kemungkinan besar dipicu oleh serangkaian insiden siber tingkat tinggi dalam beberapa tahun terakhir yang berdampak pada layanan penting dan keamanan data pribadi di Australia. Sebagaimana diidentifikasi dalam Bab II, serangan siber terhadap warga Australia dan kepentingan Australia meningkat dari tahun ke tahun. Dalam tiga tahun terakhir Australia telah menjadi sasaran sejumlah serangan siber besar yang berdampak luas terhadap masyarakat:

1) Dalam serangan terhadap perusahaan telekomunikasi *Optus* pada September 2022, peretas mengakses informasi pribadi hampir 10 juta pelanggan, termasuk nama, alamat, dan nomor paspor.
2) Bulan berikutnya, pada Oktober 2022, peretas menyerang perusahaan asuransi kesehatan *Medibank*, mengungkap informasi sensitif kesehatan dan pribadi 9,7 juta pelanggan.
3) Pada bulan Maret 2023, serangan *ransomware* terhadap perusahaan jasa keuangan *Latitude* memaksa bisnis tersebut *offline* selama lima minggu, dengan perkiraan biaya sebesar $95-105 juta.[81] Serangan tersebut menyebabkan pembobolan 14 juta catatan yang berisi data pribadi pelanggan di Australia dan Selandia Baru.
4) Pada Mei 2023 Firma Hukum *HWL Ebsworth* diretas oleh grup *ransomware ALPHV/Blackcat* yang ada kaitan dengan Rusia. Informasi hukum sensitif dari ratusan klien – termasuk lembaga pemerintah Australia – dipublikasikan online.
5) Pada bulan November 2023, sistem operator pelabuhan *DP World* diretas oleh aktor yang tidak disebutkan namanya. Penutupan paksa sistem ini menyebabkan sekitar 30.000 kontainer terdampar.[82]

[80] Neelam, R. (2023). *Lowy Institute Poll 2023 Report.* https://poll.lowyinstitute.org/report/2023/
[81] Musladin, L (2023), *As Cybercrime Evolves, Organisational Resilience Demands and Mindset Shift*
[82] Uren, *Australian Ports in a Cyber Storm*, Australian Strategic Policy Institute. https://www.aspistrategist.org.au/as-cybercrime-evolves-organisational-resilience-demands-a-mindset-shift/

6) Dalam enam bulan hingga Juni 2024, telah terjadi lebih dari 80 serangan siber yang dilaporkan secara publik terhadap bisnis Australia, yang berdampak pada ratusan ribu warga Australia.[83]

Insiden-insiden siber di atas kemungkinan besar hanyalah ujung gunung es, karena insiden-insiden berskala lebih kecil dan serangan terhadap jaringan pemerintah kemungkinan besar tidak akan mendapat perhatian publik secara luas. Meningkatnya jumlah serangan siber yang berhasil terhadap kepentingan Australia menunjukkan bahwa infrastruktur siber Australia belum optimal dalam melindungi keamanan nasional Australia. Optimalisasi infrastruktur siber harus menjadi prioritas pemerintah karena, sebagaimana telah ditetapkan, hal ini sangat penting bagi keamanan nasional. Di dunia yang semakin digital, aktor-aktor negara dan non-negara dapat mengeksploitasi kerentanan siber untuk mengganggu infrastruktur penting, mencuri informasi sensitif, dan menyebabkan kerugian yang luas.

c. Pendekatan berdasarkan analisis

Berdasarkan analisis di atas, disarankan pendekatan strategis berikut:

Pertama, Pemerintah Australia harus terus memprioritaskan pembangunan infrastruktur siber yang kuat untuk menjaga infrastruktur penting, informasi keamanan nasional, dan stabilitas perekonomian negara baik dari aktor negara maupun non-negara. Dari perspektif realis, peran utama pemerintah adalah menjamin perlindungan dan kelangsungan hidup negara dalam sistem internasional yang anarkis dimana ancaman keamanan bersifat luas dan konstan. Dalam pandangan ini, keamanan siber menjadi aspek penting dalam pertahanan negara, sama halnya dengan menjaga kekuatan militer. Pemerintah harus membangun ijin publik melalui diskusi publik yang berkelanjutan mengenai keamanan siber sebagai ancaman keamanan nasional dan harus mengalokasikan sumber daya yang tepat untuk memastikan infrastruktur siber dapat dioptimalkan. Pertimbangan juga harus diberikan untuk memperkuat partisipasi publik dalam keamanan siber.

[83] Webber Insurance Services (2024), *The Complete List of Data Breaches in Australia for 2018-2024*. https://www.webberinsurance.com.au/data-breaches-list#twentyfour

Kedua, keamanan siber harus didekati melalui kombinasi inisiatif negara dan solusi swasta. Meskipun pemerintah harus memimpin keamanan siber nasional, tidak mungkin bagi pemerintah untuk secara langsung menyediakan kemampuan keamanan siber bagi dunia usaha dan seluruh masyarakat, terutama mengingat sebagian besar jaringan siber Australia dimiliki dan dikelola oleh pemangku kepentingan swasta. Mengingat perspektif neoliberalisme, peran pemerintah dalam menyediakan infrastruktur siber sangatlah penting. Namun, harus diimbangi dengan kolaborasi yang kuat dengan sektor swasta. Hal ini mencakup pembagian informasi intelijen tentang ancaman, memberikan insentif untuk menerapkan praktik terbaik, dan menciptakan kerangka peraturan yang mendorong dunia usaha untuk berinvestasi dalam keamanan siber tanpa menghambat inovasi. Pemerintah harus bertindak sebagai fasilitator, memungkinkan sektor swasta untuk mengembangkan solusi keamanan siber yang mutakhir sambil memastikan bahwa upaya-upaya ini selaras dengan tujuan keamanan nasional.

15. Pengaruh regulasi terhadap infrastruktur siber

a. Undang-undang

Teori kontrak sosial berpendapat bahwa individu setuju untuk menyerahkan kebebasan tertentu kepada negara dengan imbalan perlindungan dan penyediaan barang publik. Dalam perspektif ini, peraturan perundang-undangan keamanan siber merupakan wujud tugas negara untuk melindungi warganya di era digital. Teori kontrak sosial memandang keamanan siber sebagai barang publik yang wajib disediakan oleh negara untuk menjamin keselamatan, privasi, dan kesejahteraan warganya. Oleh karena itu, undang-undang keamanan siber merupakan bagian penting dari infrastruktur keamanan siber suatu negara karena undang-undang tersebut menetapkan standar dan tanggung jawab untuk melindungi sistem informasi dan data. Dengan mendefinisikan kewajiban hukum individu, dunia usaha, dan lembaga pemerintah, undang-undang memastikan bahwa semua pihak memahami peran mereka dalam menjaga keamanan siber. Kejelasan ini membantu membakukan praktik keamanan, sehingga memudahkan organisasi untuk menerapkan langkah-langkah efektif dan bagi badan pengatur untuk menegakkan kepatuhan. Regulasi dapat memberikan mekanisme yang kuat

untuk mengubah insentif dan perilaku.[84] Kerangka hukum yang jelas juga dapat memberikan panduan mengenai praktik terbaik dan persyaratan keamanan minimum, sehingga mengurangi kerentanan keamanan. Perundang-undangan memungkinkan pemerintah untuk mewajibkan langkah-langkah perlindungan bagi sektor-sektor penting seperti energi, layanan kesehatan, dan keuangan, untuk memastikan sistem-sistem penting ini memiliki ketahanan terhadap serangan siber. Perundang-undangan juga memfasilitasi respons terkoordinasi terhadap insiden siber, sehingga memungkinkan tindakan cepat untuk memitigasi ancaman dan meminimalkan kerusakan.

Australia memiliki serangkaian undang-undang di tingkat Negara Bagian dan Federal yang berhubungan dengan berbagai aspek keamanan siber. Undang-undang ini umumnya diperkenalkan berdasarkan sektor per sektor, yang mencerminkan pendekatan yang berupaya menyasar sektor-sektor yang dianggap paling penting dan paling rentan. Perundang-undangan penting yang relevan di tingkat federal diuraikan dalam Tabel 1.

Nama	**Relevansi**	**Sektor**	**Badan pengelola**
Telecommunications Sector Security Reforms 2019	Kerangka perlindungan dari ancaman siber.	Telekomunikasi	Departemen Dalam Negeri
Security of Critical Infrastructure Act and Amendments 2018	Kewajiban pelaporan, rencana respons, latihan keamanan siber.	Infrastruktur penting	Departemen Dalam Negeri

[84] Shah, R (2023) *Getting Regulation Right: Approaches to Improving Australia's Cyber Security.* Australian Strategic Policy Institute https://aspi.org.au/report/getting-regulation-right-approaches-improving-australias-cybersecurity

Privacy Act 1998	Entitas harus mengambil langkah wajar untuk memastikan keamanan informasi pribadi, dan memberi tahu jika terjadi pelanggaran tertentu.	Perusahaan dengan omset >$3 juta/tahun dan beberapa organisasi lainnya.	Kantor Komisaris Informasi Australia
Corporations Act 2001	Persyaratan untuk mengirimkan pemberitahuan tentang 'situasi yang dapat dilaporkan' (misalnya pelanggaran data).	Tidak spesifik.	Komisi Sekuritas dan Investasi Australia
Crimes Act 1914	Pelanggaran komputer dan telekomunikasi.	Tidak spesifik.	Polisi Federal Australia
Online Safety Act 2021	Penyedia layanan online lebih bertanggung jawab atas keamanan online orang yang menggunakan layanan.	Tidak spesifik.	Komisaris Keamanan Elektronik

Tabel 1: Undang-undang Siber Australia

Salah satu kekuatan utama undang-undang keamanan siber Australia adalah pendekatan komprehensifnya dalam melindungi infrastruktur penting. UU SOCI dan amandemen selanjutnya mengamanatkan program manajemen risiko yang ketat dan persyaratan pelaporan insiden bagi pemilik dan operator infrastruktur penting. Hal ini memastikan bahwa entitas yang bertanggung jawab atas layanan penting seperti energi, air, dan telekomunikasi diwajibkan untuk secara proaktif mengelola risiko keamanan siber dan menerapkan kemampuan untuk merespons ancaman siber secara efektif.

Namun, seperti terlihat pada Tabel 1, undang-undang siber Australia terdapat pada sejumlah undang-undang yang berbeda, sehingga menyebabkan tumpang tindih dan kesenjangan yang mengakibatkan kurangnya kohesi. Menteri Keamanan Siber Australia, Clare O'Neil, mengatakan bahwa “kebijakan, undang-undang, dan kerangka kerja yang

tambal sulam di Australia…tidak mampu merespons tantangan era digital. Tindakan sukarela dan rencana yang dilaksanakan dengan buruk tidak akan membawa Australia ke posisi yang kami perlukan untuk berkembang dalam lingkungan yang penuh persaingan pada tahun 2030."[85] Kompleksitas dan fragmentasi lanskap peraturan menyulitkan para pemangku kepentingan untuk memahami persyaratan berbagai undang-undang dan peraturan. Kompleksitas ini dapat menimbulkan kebingungan dan tantangan kepatuhan, sehingga berpotensi menyebabkan beberapa organisasi tidak siap menghadapi ancaman siber. Menyederhanakan kerangka peraturan dapat meningkatkan kepatuhan dan meningkatkan ketahanan keamanan siber secara keseluruhan.

Sifat ancaman siber yang berkembang pesat berarti bahwa peraturan perundang-undangan dapat dengan cepat menjadi usang. Proses legislatif seringkali lebih lambat dibandingkan laju perubahan teknologi, sehingga menyulitkan peraturan untuk mengimbangi ancaman yang muncul dan vektor serangan baru. Peninjauan dan adaptasi terus-menerus terhadap undang-undang keamanan siber diperlukan untuk memastikan undang-undang tersebut tetap relevan dan efektif. Membangun mekanisme peraturan yang tangkas dan fleksibel yang dapat merespons dengan cepat perubahan lanskap ancaman siber sangat penting untuk menjaga pertahanan keamanan siber yang kuat dalam jangka panjang.

b. Standar dan Peraturan Memudahkan

Selain peraturan perundang-undangan, Australia juga memiliki sejumlah peraturan dan standar siber, yang dikeluarkan oleh berbagai bagian pemerintahan. Pedoman ini terutama dimaksudkan untuk diterapkan pada sistem pemerintahan, namun semakin banyak digunakan di sektor swasta sebagai representasi dari praktik terbaik industri.[86] Pedoman ini memberikan panduan dan saran praktis bagi organisasi untuk meningkatkan postur keamanan siber mereka tanpa adanya kekuatan hukum yang mengikat. Beberapa standar dan peraturan yang paling banyak diterapkan adalah:

[85] O'Neil dalam Commonwealth of Australia, *Australian Cyber Security Strategy 2023-2030*, *op.cit.*
[86] Shah, *op.cit.*

1) *Protective Security Policy Framework* (PSPF, Kerangka Kebijakan Keamanan Protektif): PSPF adalah serangkaian pedoman yang dirancang untuk melindungi informasi, aset, dan masyarakat pemerintah. Perjanjian ini menetapkan persyaratan wajib dan praktik terbaik di empat bidang keamanan utama: tata kelola, informasi, personel, dan keamanan fisik. Sehubungan dengan siber, PSPF mengamanatkan agar lembaga pemerintah menerapkan manajemen keamanan informasi, pengendalian akses, rencana respons insiden, dan pengendalian keamanan teknis.[87]
2) *Information Security Manual* (ISM, Manual Keamanan Informasi): ISM adalah dokumen yang dikeluarkan oleh ACSC yang memberikan pedoman dan praktik terbaik untuk manajemen keamanan informasi. Dokumen ini menguraikan kerangka keamanan siber yang dapat diterapkan suatu organisasi, dengan menggunakan kerangka manajemen risikonya, untuk melindungi sistem dan datanya dari ancaman siber. Meskipun tidak mengikat secara hukum, ISM merupakan sumber daya penting bagi lembaga pemerintah dan organisasi swasta yang ingin menyelaraskan praktik keamanan siber mereka dengan standar nasional.[88]
3) *Essential Eight*. Serangkaian strategi sukarela ini dirancang untuk membantu organisasi memitigasi insiden keamanan siber. Pedoman ini dikenal luas karena efektivitasnya dalam mengurangi risiko intrusi siber dan sangat berguna bagi usaha kecil dan menengah yang mungkin kekurangan sumber daya untuk program keamanan siber yang komprehensif.
4) *Australian Information Security Evaluation Program* (AISEP, Program Evaluasi Keamanan Informasi Australia): AISEP adalah program sertifikasi yang dikelola oleh ACSC. Ini mengevaluasi dan mensertifikasi produk dan sistem teknologi informasi dan

[87] Department of Home Affairs, *Protective Security Framework*. https://www.protectivesecurity.gov.au/about
[88] ACSC (2024), *Information Security Manual.* https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism

komunikasi untuk memastikan mereka memenuhi standar dan persyaratan keamanan. Hal ini tidak wajib, namun sangat direkomendasikan untuk produk dan sistem yang digunakan dalam lembaga pemerintah dan sistem infrastruktur penting.

Meskipun pedoman non-legislatif memberikan fleksibilitas dan kemampuan beradaptasi, pedoman tersebut juga memiliki keterbatasan. Dilihat dari perspektif realisme, pedoman siber yang bersifat sukarela kemungkinan besar tidak akan berhasil karena tidak ada mekanisme bagi negara untuk menegakkannya. Tanpa pengawasan hukum, kepatuhan terhadap pedoman ini bisa menjadi tidak konsisten, dan beberapa organisasi mungkin tidak memprioritaskan keamanan siber hingga serangan terjadi. Selain itu, sifat sukarela dari pedoman ini berarti terdapat variasi yang signifikan dalam penerapannya di berbagai sektor dan organisasi. Untuk memaksimalkan efektivitasnya, penting bagi para pemimpin industri dan badan pemerintah untuk meningkatkan kesadaran dan mendorong penerapan praktik-praktik terbaik ini secara luas, dengan menekankan manfaat jangka panjang dari langkah-langkah keamanan siber yang proaktif.

c. Pendekatan berdasarkan analisis

Berdasarkan analisis di atas, disarankan pendekatan strategis berikut:

Pertama, pemilihan standar sukarela yang dijabarkan di atas harus dijadikan suatu keharusan. Secara khusus, standar minimum keamanan siber dan kode praktik harus diamanatkan untuk memastikan tingkat perlindungan yang kuat dan konsisten di semua sektor. Menetapkan persyaratan dasar akan menciptakan kerangka kerja yang jelas dan dapat diterapkan yang wajib dipatuhi oleh semua organisasi, sehingga mengurangi kerentanan dan meningkatkan postur keamanan Australia secara keseluruhan. Jika memungkinkan, metrik atau langkah-langkah yang ingin diamanatkan oleh peraturan ini harus berbasis risiko, bukan langkah-langkah teknis tertentu. Hal ini karena tindakan teknis yang diperlukan untuk melindungi terhadap ancaman akan bergantung pada konteks individu, akan berubah seiring berjalannya

waktu, dan hanya akan efektif jika dilakukan bersama-sama dengan sumber daya manusia dan proses tindakan.[89]

Taskap ini merekomendasikan agar peraturan mengenai standar keamanan siber harus dilakukan dengan cara yang tepat sasaran dan selektif. Biaya tambahan finansial yang terkait dengan kepatuhan terhadap peraturan keamanan siber bisa jadi tinggi, dan organisasi yang lebih kecil mungkin kesulitan memenuhi tuntutan baru tanpa dukungan dan sumber daya yang memadai. Hal ini dapat menimbulkan dampak yang tidak proporsional terhadap UKM, sehingga berpotensi menghambat pertumbuhan dan daya saing mereka dalam ekonomi digital. Standar yang diamanatkan harus mencakup bidang-bidang utama seperti perlindungan data, respons insiden, dan manajemen risiko. Standar wajib harus selaras dengan standar internasional sejauh mungkin, dan tidak hanya disesuaikan dengan konteks Australia. Hal ini akan menyederhanakan kepatuhan bagi perusahaan yang beroperasi secara global. Mewajibkan standar minimum ini tidak hanya akan melindungi infrastruktur penting dan informasi sensitif namun juga mendorong budaya kesadaran dan ketahanan keamanan siber yang lebih kuat di Australia.

Kedua, undang-undang keamanan siber Australia harus ditempatkan di bawah satu payung dalam bentuk *Cyber Security Act* (Undang-Undang Keamanan Siber). Daripada menambahkan lapisan peraturan tambahan ke dalam lanskap peraturan yang ada, Undang-undang ini harus menggantikan undang-undang yang ada saat ini untuk menyederhanakan proses kepatuhan. Dengan menyatukan semua undang-undang yang relevan ke satu lokasi, redundansi dan tumpang tindih akan berkurang. Hal ini akan membuat kepatuhan lebih mudah dan lebih murah, yang berarti perundang-undangan akan lebih efektif. Undang-undang yang ada saat ini mengharuskan industri dan dunia usaha untuk melaporkan insiden ke berbagai lembaga, tergantung pada sifat insiden tersebut. Hal ini menciptakan tumpang tindih, inefisiensi dan potensi kebingungan. *Cyber Security Act* akan mengatasi masalah ini dengan mengkonsolidasikan proses dan kewajiban pelaporan serta memberikan kerangka legislatif yang jelas bagi pemerintah untuk merespons insiden siber.

[89] Shah, *op.cit.*

Dengan merumuskan pedoman yang jelas dan konsisten untuk pelaporan dan respons insiden, *Cyber Security Act* dapat mengamanatkan pelaporan insiden siber yang tepat waktu dan terstandarisasi, sehingga memastikan bahwa pelanggaran data dan serangan siber dikomunikasikan dengan cepat kepada otoritas terkait. Hal ini akan memungkinkan waktu respons yang lebih cepat, koordinasi yang lebih baik antar pemangku kepentingan, dan mitigasi ancaman siber yang lebih efektif. Selain itu, pelaporan terpusat akan meningkatkan pengumpulan dan analisis data, memberikan wawasan berharga mengenai lanskap ancaman untuk menginformasikan pengembangan kebijakan dan alokasi sumber daya. *Cyber Security Act* harus tetap fleksibel, dengan proses peninjauan berkala untuk memastikan undang-undang tersebut sejalan dengan perkembangan di lingkungan siber.

16. Dampaknya infrastruktur siber terhadap keamanan nasional.

Meskipun peraturan memainkan peranan penting dalam melindungi Australia dari serangan siber, peraturan yang terisolasi tidak akan menjaga keamanan nasional Australia. Salah satu alasan utamanya adalah sifat ancaman siber yang tidak mengenal batas negara dan tidak adanya peraturan internasional. Kaum realisme menekankan bahwa sistem internasional pada dasarnya bersifat kompetitif dan berorientasi pada bantuan diri sendiri, tanpa otoritas menyeluruh untuk menegakkan aturan atau norma di dunia maya. Hal ini mempersulit upaya keamanan bagi masing-masing negara, karena ancaman siber dapat dengan mudah melampaui batas negara, sehingga menyulitkan negara mana pun untuk mengamankan infrastruktur sibernya secara sepihak. Sifat internet yang terdesentralisasi dan global memungkinkan pelaku kejahatan, termasuk peretas yang disponsori negara dan entitas non-negara, melancarkan serangan dari mana saja, mengeksploitasi kesenjangan peraturan dan batasan yurisdiksi. Akibatnya, peraturan nasional yang paling ketat pun bisa diabaikan atau dianggap tidak efektif. Namun, mengingat tugas mendasar negara adalah melindungi masyarakatnya dari bahaya langsung, Pemerintah mempunyai kewajiban untuk mengoptimalkan infrastruktur siber Australia semaksimal mungkin untuk mengamankan negara dari serangan siber guna melindungi keamanan nasional.

Infrastruktur biasanya mengacu pada sistem perangkat keras dan perangkat lunak dasar yang penting untuk berfungsinya berbagai sektor termasuk Internet, jaringan telekomunikasi, sistem komputer, serta prosesor dan pengontrol tertanam di industri penting. Zanzig mendefinisikan infrastruktur siber sebagai “kumpulan sistem dan perangkat lunak teknologi informasi, aset fisik dan informasi, proses, dan orang-orang yang memungkinkan suatu organisasi berfungsi secara efisien dan aman di dunia maya.”[90] Menyadari betapa kompleksnya tantangan keamanan siber, infrastruktur siber di sini merujuk pada kumpulan sistem dan perangkat lunak teknologi, aset fisik dan informasi, proses, dan manusia yang memungkinkan suatu organisasi berfungsi secara efisien dan aman di dunia maya.[91] Hal ini juga mencakup kerangka kebijakan dan peraturan atau regulasi yang mendukung keamanan siber. Definisi 'infrastruktur' yang komprehensif ini menggarisbawahi keamanan siber memerlukan pendekatan holistik yang menggabungkan dimensi peraturan, prosedur, dan kebijakan untuk memastikan infrastruktur siber yang kuat dan tangguh.

Dampak luas infrastruktur siber terhadap keamanan nasional dapat dilihat melalui analisis berbasis gatra. Meskipun Australia tidak memandang kebijakan keamanan nasionalnya melalui kerangka ini, namun memberikan sudut pandang yang tepat untuk memahami potensi implikasi insiden siber terhadap masyarakat Australia.

1) **Geografi.** Infrastruktur siber memainkan peran penting dalam memantau dan mengamankan geografi Australia yang luas, memfasilitasi komunikasi dan koordinasi dalam jarak yang sangat jauh. Sistem informasi geografis (GIS) dan teknologi satelit yang terintegrasi dengan infrastruktur siber membantu dalam mengelola bencana alam, keamanan perbatasan, dan pengawasan rute maritim penting, memastikan kerangka keamanan nasional yang komprehensif.
2) **Sumber Daya Alam**. Sumber daya alam Australia yang kaya, termasuk mineral, minyak, gas, dan produk pertanian, sangat penting bagi perekonomian dan keamanan nasionalnya. Infrastruktur siber memastikan pengelolaan sumber daya yang aman dan efisien

[90] Zanzig dan Francia (2022), ‘Auditor Evaluation and Reporting on Cyber Security Risks’ dlm IGI Global *Research Anthology on Business Aspects of Cybersecurity.* Information Resources Management Association: Pennsylvania.
[91]Stewart, *op.cit.*

dengan melindungi sistem kontrol industri dari serangan siber, menjaga data terkait ekstraksi dan distribusi sumber daya, dan memastikan integritas operasional infrastruktur penting. Hal ini penting untuk mencegah gangguan ekonomi dan menjaga kemandirian energi dan sumber daya negara.

3) **Populasi**. Distribusi penduduk Australia, yang ditandai dengan pusat kota yang padat penduduknya dan wilayah pedesaan yang jarang penduduknya, memerlukan infrastruktur siber yang kuat untuk menjamin keamanan nasional. Sistem siber memfasilitasi komunikasi yang efektif, tanggap darurat, dan layanan publik di seluruh wilayah. Dengan melindungi data pribadi dan layanan publik penting dari ancaman siber, infrastruktur siber membantu menjaga stabilitas sosial dan kepercayaan publik.

4) **Ideologi**. Langkah-langkah keamanan siber menjamin integritas sistem pemilu, mencegah misinformasi dan campur tangan pihak asing, serta melindungi kebebasan berpendapat secara online. Dengan mengamankan platform digital dan jaringan komunikasi, Australia dapat menjunjung tinggi prinsip-prinsip ideologisnya dan menjaga kepercayaan publik terhadap proses demokrasi.

5) **Politik.** Stabilitas politik di Australia didukung oleh infrastruktur siber yang aman yang melindungi operasi pemerintah, jaringan komunikasi, dan data sensitif dari ancaman siber. Memastikan keamanan siber pada institusi politik mencegah spionase, pelanggaran data, dan serangan siber yang dapat mengganggu stabilitas pemerintahan dan mengikis kepercayaan publik.

6) **Ekonomi**. Perekonomian Australia sangat bergantung pada infrastruktur digital untuk perdagangan, perbankan, dan industri. Infrastruktur siber sangat penting untuk melindungi aktivitas ekonomi dari ancaman siber, memastikan integritas transaksi keuangan, menjaga kekayaan intelektual, dan menjaga kelangsungan operasi bisnis. Lingkungan siber yang aman mendorong stabilitas dan pertumbuhan ekonomi.

7) **Sosial dan Budaya**. Langkah-langkah keamanan siber dapat membantu mencegah pelecehan online, penindasan maya, dan

penyebaran konten berbahaya, serta memastikan ruang digital yang aman untuk ekspresi budaya dan kohesi sosial. Melindungi platform-platform ini akan mendukung masyarakat yang berketahanan dan bersatu, yang sangat penting bagi keamanan nasional.

8) **Pertahanan dan Keamanan**. Pertahanan dan keamanan Australia semakin bergantung pada infrastruktur siber yang canggih untuk melindungi operasi militer dan penegakan hukum. Tindakan keamanan siber melindungi komunikasi pertahanan, sistem kendali, dan jaringan intelijen dari ancaman siber. Dengan memastikan integritas dan ketersediaan sistem siber yang terkait dengan pertahanan, Australia dapat mempertahankan kemampuan pertahanan nasionalnya dan melindungi terhadap ancaman perang konvensional dan siber.

a. Kebijakan dan Strategi Pemerintah

Pentingnya peraturan yang kuat telah dijelaskan sebelumnya dalam bab ini. Aspek penting lainnya dalam infrastruktur siber Australia adalah kebijakan atau strategi pemerintah. Kebijakan dan strategi inilah yang menentukan cara pemerintah bekerja sama dengan dunia usaha dan masyarakat Australia untuk melindungi negara dari serangan siber. Kebijakan keamanan siber Australia dirancang untuk melindungi infrastruktur digital negara tersebut, meningkatkan ketahanan sektor-sektor penting, dan mendorong ekonomi digital yang aman dan berkembang. Landasan upaya ini adalah *Australian Cyber Security Strategy* (ACSS) 2023-30, yang menguraikan pendekatan komprehensif untuk mengelola risiko siber dan mengamankan ruang siber negara tersebut.

ACSS merupakan komitmen kebijakan yang kuat dari Pemerintah Australia untuk mengelola ancaman siber terhadap keamanan nasional Australia. ACSS adalah 'peta jalan' yang akan mewujudkan visi Pemerintah untuk menjadi pemimpin dunia dalam keamanan siber pada tahun 2030. Enam perisai ACSS yang dijelaskan dalam Bab II berpusat pada warga negara dan dunia usaha Australia dan menunjukkan komitmen Pemerintah untuk melakukan pendekatan terhadap keamanan siber sebagai upaya seluruh bangsa. Pemerintah mengeluarkan *Action Plan* (rencana aksi) ACSS yang menguraikan inisiatif yang akan dilaksanakan dalam jangka waktu 2023-25

untuk melaksanakan strategi tersebut. Hal ini mencakup tindakan spesifik yang berfokus pada memperkuat landasan keamanan siber. *Action Plan* dirancang dinamis dan akan diperbarui setiap dua tahun sekali.

Meskipun ACSS disambut baik secara luas, tercatat bahwa paling banyak delapan dari 48 tindakan yang ditentukan dalam strategi ini merupakan inisiatif baru. Yang lain sudah diperkenalkan, atau sudah dicoba sebelumnya.[92] Memang benar, upaya Australia untuk menerapkan kebijakan keamanan siber telah mencapai keberhasilan yang beragam, dengan penerapan strategi sebelumnya yang tidak merata dan tidak efektif. Meskipun memiliki kerangka kerja yang komprehensif dan ambisius, ACSS mempunyai sejumlah kelemahan potensial. Salah satu kekhawatirannya adalah meskipun strategi ini menyoroti pentingnya kolaborasi, mekanisme untuk mencapainya tidak terdefinisi dengan baik, sehingga berpotensi menyebabkan kesenjangan dalam koordinasi dan pelaksanaan. Kedua, fokus strategi ini pada kewajiban pelaporan insiden menimbulkan pertanyaan tentang potensi penyalahgunaan informasi yang dilaporkan oleh regulator, yang mungkin menghalangi dunia usaha untuk sepenuhnya transparan mengenai insiden siber. Tanpa perlindungan yang jelas, perusahaan mungkin enggan membagikan informasi penting, sehingga melemahkan strategi tersebut.[93] Terakhir, strategi ini pada dasarnya bergantung pada upaya sukarela untuk mengatasi keamanan siber, dibandingkan dengan standar yang diamanatkan dan penegakan hukum yang kuat. Hal ini berarti bahwa perusahaan-perusahaan besar, yang menyimpan sejumlah besar data sensitif dan memiliki pengaruh signifikan terhadap praktik keamanan siber, tidak cukup terdorong untuk mematuhi standar keamanan yang ketat. Tanpa langkah-langkah wajib dan akuntabilitas, terdapat risiko bahwa entitas-entitas ini tidak akan memprioritaskan keamanan siber semaksimal mungkin, sehingga berpotensi menjadikan sektor-sektor penting rentan terhadap ancaman siber.

92 Bareja dan Caples (2023), *Australia's New Cybersecurity Strategy Tackles the Tough Issues.* Australian Strategic Policy Institute https://www.aspistrategist.org.au/australias-new-cybersecurity-strategy-tackles-the-tough-issues/

93 Macpherson dkk (2023), *Australia's Cyber Security – A Bold Regulatory Reform Agenda* https://www.ashurst.com/en/insights/australias-cyber-strategy-a-bold-regulatory-reform-agenda/

b. Pendekatan berdasarkan analisis: Kebijakan dan Strategi Pemerintah

Berdasarkan analisis di atas, disarankan pendekatan strategis berikut:

Pertama, Pemerintah Australia harus mengambil langkah-langkah untuk mendapatkan dukungan bipartisan terhadap pendekatan bersama terhadap keamanan siber. Hal ini dapat dicapai dengan menekankan sifat non-partisan dari keamanan nasional dan menjadikan keamanan siber sebagai isu penting yang melampaui perpecahan politik. Keterlibatan dalam proses pembuatan kebijakan yang transparan dan inklusif, yang melibatkan perwakilan dari semua partai politik besar sejak awal, dapat menumbuhkan rasa kepemilikan dan komitmen bersama. Selain itu, pembentukan komite bipartisan untuk mengawasi pengembangan dan penerapan kebijakan keamanan siber dapat memastikan bahwa beragam perspektif dipertimbangkan, sehingga menghasilkan solusi yang lebih kuat dan diterima secara luas. Dengan menumbuhkan lingkungan politik yang kooperatif, pemerintah dapat menciptakan kerangka kerja yang stabil dan bertahan lama untuk mengatasi tantangan keamanan siber, yang pada akhirnya meningkatkan ketahanan nasional terhadap ancaman siber.

Kedua, Pemerintah Australia harus memperjelas bagaimana implementasi Strategi Keamanan Siber Australia akan dilacak dan dijelaskan kepada publik. Suatu strategi harus berhasil diterapkan agar efektif, dan komitmen terhadap pelaporan rutin dan transparansi sangatlah penting. Dengan menetapkan ukuran yang jelas dan menetapkan jadwal yang konsisten untuk memperbarui kemajuan, Pemerintah dapat meyakinkan masyarakat akan komitmennya terhadap tujuan yang telah ditetapkan. Transparansi ini tidak hanya membangun kepercayaan publik namun juga memastikan akuntabilitas, memungkinkan para pemangku kepentingan untuk memantau kemajuan dan meminta pertanggungjawaban pemerintah dalam mencapai tujuan keamanan sibernya. Komunikasi rutin dan laporan kemajuan yang terperinci akan menekankan komitmen pemerintah terhadap perbaikan berkelanjutan dan kemampuannya beradaptasi terhadap ancaman siber yang muncul.

Ketiga, dan terkait dengan saran di atas, Pemerintah harus berkomitmen terhadap siklus strategi siber dua tahunan. Meskipun Pemerintah

telah menyatakan akan meninjau *Action Plan* setiap dua tahun, rencana ini harus diperluas hingga mencakup tinjauan komprehensif dan penerbitan ulang strategi siber Australia. Baru-baru ini, Pemerintah Australia berkomitmen untuk menyusun Strategi Pertahanan Nasional setiap dua tahun, dengan mengakui bahwa lingkungan geo-strategis yang berubah dengan cepat memerlukan ketangkasan dalam respons kebijakan. Komitmen yang sama juga harus diperluas ke strategi siber, dimana lanskap strategis dan teknologi berkembang lebih cepat lagi. Dengan menerapkan siklus dua tahunan, Pemerintah dapat memastikan bahwa strategi sibernya tetap terkini, responsif, dan selaras dengan kemajuan dan ancaman teknologi terkini. Pendekatan proaktif ini akan membekali Australia dengan lebih baik dalam mengatasi tantangan siber yang muncul dan mempertahankan postur keamanan siber yang kuat dan tangguh.

Keempat, Pemerintah Australia harus mengembangkan Strategi Keamanan Nasional. Strategi Keamanan Nasional akan memastikan bahwa sumber daya dan perhatian keamanan nasional dialokasikan secara tepat, dan mengintegrasikan keamanan siber ke dalam kerangka yang lebih luas. Strategi ini harus melengkapi strategi siber yang ada, memberikan konteks menyeluruh yang menempatkan ancaman siber dalam lanskap keamanan nasional yang lebih luas. Dengan mengkontekstualisasikan ancaman siber dan tantangan keamanan lainnya, Strategi Keamanan Nasional akan menyoroti sifat saling terkait dari ancaman-ancaman tersebut dan memastikan ancaman-ancaman ini ditangani dengan urgensi yang diperlukan. Pendekatan holistik ini akan memfasilitasi upaya terkoordinasi di berbagai sektor, meningkatkan efektivitas dan ketahanan keseluruhan postur keamanan Australia.

c. Struktur Tata Kelola Siber

Struktur tata kelola siber Australia merupakan aspek penting dari infrastruktur siber Australia yang mendukung penerapan peraturan, kebijakan, dan strategi pemerintah. Dalam konteks ini yang dimaksud dengan struktur tata kelola adalah peran, tanggung jawab, dan hubungan antar lembaga pemerintah. Dimulai dari tingkat pemerintahan terpilih, Pemerintah saat ini telah menunjukkan komitmen terkuat terhadap keamanan siber dibandingkan pemerintahan mana pun sejauh ini, dengan penunjukan menteri keamanan siber setingkat kabinet. Kekuatan utama dari adanya menteri yang berdedikasi

terhadap keamanan siber adalah kepemimpinan yang terfokus dan pengawasan strategis yang diberikan terhadap upaya keamanan siber nasional. Menteri ini membantu memfokuskan perhatian dan sumber daya pada isu penting ini dan mendorong pendekatan yang lebih terpadu dan kohesif untuk mengatasi ancaman siber.

Meskipun demikian, ada beberapa faktor yang membatasi efektivitas peran menteri ini. Salah satu keterbatasan utama adalah kenyataan bahwa mendapatkan pendanaan, personel, dan sumber daya lainnya yang memadai masih merupakan tantangan. Di Australia, keamanan siber bersaing dengan isu-isu kebijakan publik lainnya untuk mendapatkan perhatian dan sumber daya. Isu-isu seperti biaya hidup, pengelolaan ekonomi dan kesejahteraan sosial, bukan isu keamanan nasional, cenderung menjadi fokus kampanye pemilu. Namun, dampak luas dari insiden *Optus* dan *Medibank* menjadikan keamanan siber sebagai isu yang menjadi perhatian publik, sehingga meningkatkan dukungan umum terhadap pendanaan dan tindakan respons lainnya. Keterbatasan penting yang kedua adalah efektivitas pekerjaan yang dilakukan oleh Menteri akan dipengaruhi oleh faktor politik dan perubahan dalam pemerintahan. Seiring dengan perubahan kepemimpinan politik, mungkin terjadi pergeseran fokus kebijakan, prioritas, dan kesinambungan inisiatif. Secara khusus, tidak ada jaminan bahwa Pemerintahan di masa depan akan memasukkan Menteri Keamanan Siber ke dalam kabinetnya atau memberikan dukungan anggaran berkelanjutan untuk inisiatif yang diperkenalkan oleh Menteri dan Pemerintah saat ini. Hal ini dapat menciptakan ketidakpastian dan berdampak pada perencanaan strategis jangka panjang yang diperlukan untuk langkah-langkah keamanan siber yang kuat. Memastikan bahwa keamanan siber tetap menjadi prioritas yang konsisten di berbagai pemerintahan adalah hal yang penting untuk mempertahankan postur keamanan siber nasional yang tangguh.

Ciri kedua dalam struktur tata kelola siber Australia yang baru diperkenalkan baru-baru ini adalah posisi Koordinator Siber. Peran utama Koordinator adalah mengelola respons insiden siber di tingkat nasional. Jika terjadi insiden siber, Koordinator akan bekerja dengan lembaga pemerintahan untuk mendukung respons yang efisien. Koordinator Siber adalah titik kontak utama bagi berbagai pemangku kepentingan, termasuk lembaga pemerintah,

mitra sektor swasta, dan mitra internasional. Koordinasi terpusat ini membantu menyederhanakan upaya keamanan siber, mengurangi redundansi, dan meningkatkan efisiensi respons terhadap ancaman siber. Koordinator ini didukung oleh Kantor Nasional untuk Keamanan Siber, sebuah entitas yang berlokasi di Departemen Dalam Negeri.

Ancaman siber bersifat kompleks sehingga seringkali memerlukan upaya terkoordinasi dari berbagai sektor seperti keuangan, layanan kesehatan, energi, dan telekomunikasi. Koordinator dapat menjembatani sektor-sektor ini, mendorong pertukaran praktik terbaik, intelijen ancaman, dan strategi respons insiden. Pendekatan kolaboratif ini membantu membangun kerangka keamanan siber nasional yang lebih tangguh, dengan memanfaatkan kekuatan dan keahlian berbagai industri. Koordinator memberikan arahan dan pengawasan strategis untuk pengembangan kebijakan keamanan siber di seluruh pemerintahan. Hal ini termasuk mendukung penguatan sistem Pemerintah Australia dan bekerja sama dengan industri untuk meningkatkan ketahanan siber.[94]

Namun, meskipun Koordinator bertanggung jawab mengawasi dan mengoordinasikan upaya keamanan siber, posisinya tidak memiliki kewenangan langsung untuk menegakkan kepatuhan atau mengamanatkan tindakan di seluruh departemen pemerintah dan entitas sektor swasta. Keterbatasan ini menghambat kemampuan koordinator untuk menerapkan strategi keamanan siber yang kohesif dan komprehensif secara efektif. Efektivitas Koordinator semakin dibatasi oleh kompleksitas koordinasi antar pemerintahan dan bisnis yang terdesentralisasi dan beragam. Sektor dan organisasi berbeda mempunyai prioritas, kemampuan, dan tingkat kematangan keamanan siber yang berbeda pula. Menyelaraskan elemen-elemen yang berbeda ini ke dalam pendekatan nasional yang kohesif merupakan sebuah tantangan. Koordinator harus mengatasi kompleksitas ini, membina kerja sama dan memastikan bahwa semua pemangku kepentingan berkomitmen terhadap tujuan keamanan siber bersama.

[94] Department of Home Affairs, *Cyber Coordinator.* https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/cyber-coordinator

Keterbatasan lain dari peran Koordinator Siber adalah keputusan Pemerintah untuk mengisi posisi tersebut dengan perwira militer yang diperbantukan. Menurut Seebeck, keputusan ini menimbulkan pertanyaan mengenai komitmen pemerintah terhadap keamanan siber.[95] Siber adalah masalah yang abadi dan tidak akan 'diselesaikan' hanya dengan penempatan militer. Berinvestasi dalam membangun dan mengidentifikasi talenta di sektor siber, bisnis, atau teknologi akan membawa perspektif yang lebih seimbang terhadap peran Koordinator. Hal ini berarti posisi tersebut kecil kemungkinannya untuk menjadi sasaran pertarungan birokrasi dan akan membantu membangun keahlian sipil.

Keamanan siber telah menjadi portofolio yang sangat luas di pemerintahan Australia. Di antara entitas yang bertanggung jawab adalah badan kebijakan di Kementerian Dalam Negeri (yang mencakup Kantor Keamanan Siber Nasional); terdapat badan operasional, yang mencakup ASD dan ACSC, Kepolisian Federal Australia, dan *Australian Transaction Reports and Analysis Centre* (AUSTRAC, Pusat Pelaporan dan Analisis Transaksi Australia); dan ada dimensi internasional dengan Departemen Luar Negeri dan Perdagangan. Departemen Pertahanan juga bertanggung jawab atas aspek-aspek postur siber Australia yang berkaitan dengan peperangan. Rentang peran dan tanggung jawab yang rumit ini dapat menimbulkan persaingan dan perebutan kekuasaan antar departemen yang bertanggung jawab.[96] Meskipun upaya-upaya dilakukan untuk melakukan koordinasi antar departemen, silo dan duplikasi pasti akan terjadi. Tanggung jawab siber dari departemen terkait disajikan di Tabel 2.

Departemen pemerintahan	**Tanggung Jawab Siber**
ASD	Memimpin urusan operasional keamanan siber nasional melalui ACSC. Menyediakan sumber daya teknis dan keahlian selama insiden siber nasional, menganalisis dan

[95] Seebeck, L (2023). *The Choice of Cyber Coordinator Reflects Weakened Cyber Capability*. https://strategicanalysis.org/the-choice-of-cyber-coordinator-reflects-weakened-cyber-capability/
[96] *ibid*

	berbagi informasi tentang ancaman siber, dan mengoordinasikan pesan publik terkait insiden siber.
Departemen Dalam Negeri	Mengawasi kebijakan dan strategi keamanan siber nasional, memimpin perbaikan kebijakan keamanan siber di seluruh pemerintahan dan industri, dan mengelola Kerangka Kebijakan Keamanan Protektif. Juga termasuk Kantor Nasional untuk Keamanan Siber, yang mengoordinasikan upaya untuk meningkatkan ketahanan siber nasional dan mengelola risiko siber.
ACSC	Sebagai bagian dari ASD, ACSC memberikan nasihat dan bantuan keamanan siber kepada semua tingkat pemerintahan, bisnis, dan individu. Hal ini meningkatkan ketahanan siber melalui pembagian intelijen ancaman dan kolaborasi dengan mitra internasional.
Badan Transformasi Digital	Mendorong transformasi digital di seluruh pemerintahan dengan memberikan kepemimpinan strategis dan kebijakan. Mengembangkan dan mengawasi implementasi inisiatif digital dan memastikan layanan digital pemerintah aman.
Attorney General's Department (Departemen Kejaksaan Agung)	Mengembangkan dan memelihara kerangka hukum dan kebijakan terkait kejahatan siber. Mendukung investigasi dan penuntutan kejahatan siber dan membangun kapasitas melalui program bimbingan dan pelatihan.
Badan Penanggulangan Darurat Nasional	Mendukung koordinasi respons nasional terhadap insiden keamanan siber dan berkolaborasi dengan Koordinator Siber untuk manajemen konsekuensi yang efektif.

Polisi Federal Australia	Menyelidiki kejahatan siber dan berkolaborasi dengan ASD serta lembaga lain dalam merespons insiden keamanan siber nasional. Memberikan dukungan untuk investigasi kriminal terkait keamanan siber.
Departemen Perdana Menteri dan Kabinet	Memberikan kepemimpinan dan koordinasi menyeluruh untuk upaya keamanan siber nasional dan memastikan keselarasan dengan kebijakan dan strategi keamanan nasional yang lebih luas.
Departemen Pertahanan	Bekerja erat dengan ASD dan badan-badan lain untuk melindungi jaringan Pertahanan dan sistem informasi dari ancaman siber. Bertanggung jawab atas keamanan komunikasi militer dan infrastruktur teknologi informasi.
AUSTRAC	Memantau transaksi keuangan untuk mengidentifikasi dan mencegah pencucian uang dan pendanaan terorisme. Bekerja dengan lembaga lain untuk memerangi kejahatan keuangan yang dimungkinkan oleh dunia maya dan meningkatkan keamanan sistem keuangan terhadap ancaman siber.
Departemen Luar Negeri dan Perdagangan	Bekerja secara internasional untuk mempromosikan norma-norma dunia maya dan berkolaborasi dengan negara-negara lain untuk meningkatkan keamanan siber global. Juga mendukung kepentingan Australia dalam diskusi dan perjanjian kebijakan siber internasional.

Tabel 2: Tanggung Jawab Siber Dari Departemen Terkait

Keterlibatan banyak departemen dapat menyebabkan upaya terfragmentasi dan tantangan dalam koordinasi. Karena masing-masing lembaga bertanggung jawab atas berbagai aspek keamanan siber, maka sulit untuk memastikan pendekatan yang kohesif dan terpadu. Fragmentasi ini dapat menghambat komunikasi efektif dan pembagian informasi penting secara cepat selama terjadinya insiden siber. Ketika banyak entitas terlibat, akan sulit untuk menentukan akuntabilitasnya. Menentukan departemen mana yang bertanggung jawab atas kegagalan atau keberhasilan tertentu bisa jadi rumit, sehingga berpotensi menimbulkan kesenjangan dalam tanggung jawab.

Distribusi sumber daya di berbagai departemen dapat melemahkan fokus dan efektivitas upaya keamanan siber. Hal ini juga berlaku dalam implementasi kebijakan, dimana memiliki banyak departemen yang bertanggung jawab untuk merancang dan menerapkan berbagai aspek kebijakan siber berisiko menimbulkan inkonsistensi dan fragmentasi, sehingga mempersulit kepatuhan terhadap kebijakan-kebijakan tersebut dan mewujudkan hasil yang diinginkan.

a. Pendekatan berdasarkan analisis: Struktur Tata Kelola Siber

Berdasarkan analisis di atas, disarankan pendekatan strategis berikut

Pertama, Koordinator Siber harus ditempatkan pada posisi yang kompetitif, selaras dengan masa jabatan kepala lembaga dan departemen (biasanya lima tahun di Australia). Jabatan yang diisi oleh perwira militer pada penugasan tidak memberikan stabilitas dan kesinambungan yang diperlukan untuk peran penting tersebut. Penunjukan dengan jangka waktu tetap akan memastikan koordinator dapat menetapkan strategi jangka panjang dan menyelesaikannya hingga selesai, daripada menjadi sasaran gangguan yang terkait dengan seringnya pergantian karyawan. Stabilitas ini penting untuk membangun hubungan yang kuat dengan mitra domestik dan internasional, dan mempertahankan pendekatan strategis yang konsisten terhadap ancaman siber yang terus berkembang. Proses seleksi untuk Koordinator harus kompetitif dan terbuka bagi berbagai kandidat dari berbagai kalangan pemerintahan dan dunia usaha.

Kedua, kewenangan penegakan hukum dari Koordinator Siber harus ditingkatkan. Koordinator harus memiliki kewenangan untuk menegakkan kepatuhan terhadap peraturan dan standar keamanan siber tertentu, khususnya yang berlaku pada infrastruktur penting dan lembaga pemerintah. Memberikan kemampuan untuk menjatuhkan hukuman, mewajibkan tindakan perbaikan, dan memastikan kepatuhan terhadap protokol keamanan akan memungkinkan Koordinator untuk secara signifikan meningkatkan ketahanan Australia terhadap ancaman siber.

Ketiga, struktur Kantor Keamanan Siber Nasional harus diubah agar menjadi pendekatan yang sepenuhnya melibatkan departemen terkait. Sebagaimana diuraikan, koordinasi upaya keamanan siber tersebar di sejumlah lembaga berbeda, sehingga berpotensi menimbulkan tumpang tindih

dan kesenjangan tanggung jawab. Meskipun tidak mungkin atau praktik untuk membentuk departemen keamanan siber yang baru, Kantor Keamanan Siber Nasional harus diperkuat dengan mengintegrasikan perwakilan dari semua departemen pemerintah terkait. Hal ini harus mencakup perwakilan yang memiliki senioritas yang cukup untuk dapat mengambil keputusan dan memberikan rekomendasi. Pendekatan terpadu ini berbiaya rendah, dan akan memfasilitasi pertukaran informasi yang lebih baik, menyederhanakan proses pengambilan keputusan, dan memastikan respons yang terkoordinasi terhadap ancaman siber.

b. Tenaga Kerja Siber

Walaupun Australia adalah salah satu negara yang paling aman dari perspektif siber, Australia telah mengalami kekurangan tenaga kerja siber selama beberapa dekade yang meningkatkan risiko pelanggaran siber. Permasalahan ini terus meningkat dari tahun ke tahun, dan paling parah di sektor pemerintahan karena gaji yang lebih rendah dan persyaratan izin keamanan yang berat.[97] *ISC2 Cyber Security Workforce Study 2023* mencatat kesenjangan tenaga kerja keamanan siber global telah mencapai rekor tertinggi, dengan kekurangan 4 juta tenaga profesional.[98] *Cyber Security Sector Competiveness Plan AustCyber* tahun 2023 menemukan bahwa tenaga kerja keamanan siber Australia akan membutuhkan tambahan 85.000 profesional pada tahun 2030, meningkat sebesar 66 persen dari angkatan kerja tahun 2023.[99] Hal ini memerlukan hampir 5.000 orang untuk dipekerjakan setiap tahun selama tujuh tahun ke depan, dengan asumsi perkiraan tenaga kerja tetap stabil.

Keamanan siber adalah bidang dinamis yang memerlukan pembelajaran dan adaptasi berkelanjutan terhadap teknologi baru dan ancaman yang muncul. Namun, program pendidikan yang ada seringkali kesulitan untuk mengimbangi perubahan-perubahan ini, sehingga

---

[97] Bareja dan Caples, *op. cit.*
[98] ISC2 (2023), *ISC2 Reveals Growth in Global Cybersecurity Workforce, But Record-Breaking Gap of 4 Million Cybersecurity Professionals Looms*. https://www.isc2.org/Insights/2023/10/ISC2-Reveals-Workforce-Growth-But-Record-Breaking-Gap-4-Million-Cybersecurity-Professionals
[99] AustCyber (2024), *AustCyber Report Reveals Local Cyber Security Sector is at a Pivotal Juncture. as Global Competitiveness Slips and the Skills Gap Widens.* https://www.austcyber.com/sites/default/files/2024-05/SCP%20media%20release%20%282%29.pdf

mengakibatkan angkatan kerja mungkin kekurangan keterampilan dan pengetahuan yang diperlukan untuk menangani ancaman siber saat ini dan di masa depan. Menurut *AustCyber*, 74% profesional keamanan siber melaporkan kurangnya pekerja berkualitas yang diperlukan untuk memastikan perlindungan siber.[100] Tingginya permintaan akan tenaga profesional keamanan siber membuat mereka sering dihadapkan pada banyak peluang kerja, baik di dalam negeri maupun internasional, sehingga menyebabkan tingginya tingkat turnover. Organisasi harus bersaing tidak hanya untuk menarik talenta terbaik namun juga untuk mempertahankan mereka.

Keberagaman dan inklusi dalam angkatan kerja keamanan siber adalah bidang lain yang memerlukan perhatian. Bidang keamanan siber secara historis didominasi oleh laki-laki, dan partisipasi yang lebih besar dari perempuan dan kelompok lain yang kurang terwakili harus didorong. Menurut data Sensus 2021, hanya 17% tenaga kerja keamanan siber di Australia adalah perempuan.[101] Keberagaman tenaga kerja tidak hanya meningkatkan jumlah pekerja, namun juga memberikan perspektif dan pendekatan berbeda dalam penyelesaian masalah, sehingga dapat meningkatkan efektivitas langkah-langkah keamanan siber secara keseluruhan.

c. Pendekatan berdasarkan analisis: Tenaga Kerja Siber

Berdasarkan analisis di atas, disarankan pendekatan strategis berikut:

Pertama, perlu adanya upaya yang disengaja untuk merekrut tenaga kerja siber yang lebih beragam di Australia. Hal ini dapat dicapai melalui program penjangkauan dan kemitraan yang ditargetkan dengan lembaga pendidikan, organisasi profesi, dan kelompok masyarakat untuk menarik individu dari berbagai latar belakang, termasuk perempuan, minoritas, dan kelompok yang kurang terwakili. Selain itu, pemberian beasiswa, magang, dan program bimbingan yang khusus ditujukan kepada kelompok-kelompok ini dapat membantu menjembatani kesenjangan dan mendorong masuknya mereka ke bidang keamanan siber. Mempromosikan budaya inklusivitas dalam

[100] *Ibid.*
[101] Austech Media (2023), *Women Critical to Future of Australia's Cyber Security Workforce.* https://www.techbusinessnews.com.au/news/women-critical-to-future-of-australias-cyber-security-workforce/#google_vignette

organisasi dan memastikan bahwa kebijakan keberagaman dan inklusi diterapkan dan dipantau secara aktif dapat lebih meningkatkan upaya-upaya ini. Dengan menciptakan lingkungan yang inklusif, bidang keamanan siber dapat menarik dan mempertahankan lebih banyak talenta, yang mana hal ini penting untuk mengatasi kekurangan tenaga kerja. Tim yang beragam membawa perspektif dan pendekatan pemecahan masalah yang berbeda, sehingga meningkatkan efektivitas langkah-langkah keamanan siber secara keseluruhan.

Kedua, pertimbangan harus diberikan untuk membina kemitraan antara industri dan akademisi untuk memberikan peningkatan keterampilan yang konsisten bagi orang-orang yang telah memasuki dunia kerja siber. Kemitraan ini dapat menciptakan peluang pembelajaran berkelanjutan melalui program pelatihan bersama, lokakarya, dan sertifikasi. Pakar industri dapat berkolaborasi dengan institusi akademis untuk mengembangkan program yang mencerminkan tren dan teknologi keamanan siber terkini, sehingga memastikan bahwa para profesional tetap memiliki pengetahuan dan keterampilan terkini. Selain itu, kolaborasi semacam ini dapat memfasilitasi inisiatif penelitian dan pengembangan yang memajukan bidang keamanan siber, serta memberikan solusi praktis terhadap ancaman yang muncul.

Ketiga, AI harus dimanfaatkan untuk membantu mengisi kesenjangan keterampilan. Alat berbasis AI dapat mengotomatiskan tugas-tugas rutin keamanan siber, seperti deteksi ancaman, respons insiden, dan penilaian kerentanan, sehingga memungkinkan para profesional untuk fokus pada aktivitas yang lebih kompleks dan strategis. AI juga dapat digunakan untuk meningkatkan program pelatihan dengan memberikan pengalaman pembelajaran yang dipersonalisasi dan simulasi virtual yang meniru ancaman siber di dunia nyata. Dengan mengintegrasikan AI ke dalam operasi dan pendidikan keamanan siber, Australia dapat memaksimalkan efisiensi dan efektivitas tenaga kerja yang ada, mengatasi kekurangan keterampilan sekaligus meningkatkan postur keamanannya secara keseluruhan.

d. Teknis

Meskipun Taskap ini difokuskan pada aspek non-teknis infrastruktur siber Australia, penting untuk mengetahui sisi teknis dari keamanan siber,

karena pada kenyataannya, sistem teknis TIK-lah yang pada akhirnya menentukan kerentanan suatu entitas terhadap gangguan siber. Jika semua pemilik sistem TIK menerapkan langkah-langkah keamanan siber yang ketat, maka sistem ini akan menjadi target yang lebih sulit bagi pelaku siber jahat. Namun, karena basis teknologi informasi Australia dirancang, dikembangkan, dipelihara atau dikendalikan oleh industri swasta, bukan oleh pemerintah, maka skala, cakupan, kerentanan dan peluangnya tidak terlihat jelas.

Dari perspektif keamanan nasional, aspek teknis infrastruktur siber dapat dipecah menjadi dua dimensi: pelanggaran/ofensif dan pertahanan/defensif. Perspektif realisme berpendapat bahwa memiliki kemampuan serangan siber yang kuat diperlukan untuk pencegahan. Kemampuan untuk melancarkan serangan siber balasan dapat menghalangi musuh untuk memulai tindakan siber. Konsep ini mirip dengan teori pencegahan (*deterence theory)*, dimana ancaman serangan balasan yang signifikan dapat mencegah serangan awal. Kemampuan siber yang bersifat ofensif juga dipandang oleh teori realisme sebagai alat untuk memproyeksikan kekuatan dan pengaruh dalam hubungan internasional. Hal ini merupakan sarana untuk memperoleh keuntungan strategis tanpa menggunakan kekuatan militer konvensional.

Kemampuan siber yang bersifat pelanggaran berada dalam bidang operasi intelijen dan jarang dibahas secara publik. Di Australia, proyek REDSPICE mencakup peningkatan tiga kali lipat kemampuan serangan siber ASD, namun tidak ada informasi tersedia mengenai dampaknya. Direktur Jenderal ASD dalam pidatonya pada tahun 2021 menyatakan bahwa 'sebagai bagian dari upaya ASD secara menyeluruh untuk membela Australia...kemampuan siber ofensif digunakan untuk menyerang balik penjahat siber di luar negeri yang melakukan aktivitas jahat."[102] Beliau mengatakan bahwa teknik yang digunakan oleh ASD termasuk 'SMS palsu', 'operasi online rahasia dan kemampuan serangan jaringan komputer.'[103] Diketahui juga secara publik bahwa ASD bekerja sama dengan Polisi Federal Australia untuk menargetkan penjahat siber di luar negeri dalam program yang

[102] Noble, *op.cit.*
[103] *Ibid.*

dikenal sebagai *'Hack the Hackers'*. Inisiatif ini bertujuan untuk memburu dan mengganggu operasi sindikat kejahatan siber internasional, memanfaatkan intelijen dan kemampuan siber ofensif untuk melawan ancaman siber.[104]

Kemampuan siber defensif merupakan komponen yang sama pentingnya dari sisi teknis infrastruktur siber Australia, namun bukan merupakan domain eksklusif pemerintah. Neoliberalisme menyoroti pentingnya kerja sama antara sektor publik dan swasta. Mengingat sebagian besar infrastruktur penting dan kemampuan siber Australia dikelola oleh entitas swasta, pertahanan siber yang efektif memerlukan kolaborasi antara pemerintah dan dunia usaha. Kapabilitas siber defensif Australia menjangkau spektrum publik-swasta. Dari sudut pandang teknis, langkah-langkah seperti enkripsi yang kuat, *patching* dan pembaruan rutin, autentikasi multi-faktor, sistem deteksi intrusi, dan praktik pengkodean yang aman merupakan hal mendasar untuk melindungi aset digital. Pertahanan ini menciptakan keamanan berlapis, sehingga lebih sulit bagi penyerang untuk menembus sistem. Namun, musuh siber terus mengembangkan taktik dan teknik baru untuk melewati langkah-langkah keamanan yang ada, sehingga memerlukan kewaspadaan dan adaptasi terus-menerus. Untuk mengimbangi ancaman yang terus berkembang ini, diperlukan investasi berkelanjutan dalam penelitian dan pengembangan, serta pembaruan langkah-langkah dan teknologi keamanan siber secara terus-menerus.

e. Pendekatan berdasarkan analisis: Teknis

Berdasarkan analisis di atas, disarankan pendekatan strategis berikut:

Pertama, dari sudut pandang pelanggaran, Australia harus terus mengembangkan cara untuk mengidentifikasi dan menghubungkan serangan siber dengan aktor tertentu. Kemampuan penyerang untuk mengaburkan asal usul mereka menjadikan hal ini sebagai tugas yang menantang, dan kesalahan atribusi berpotensi menyebabkan kesalahan penargetan dan eskalasi konflik. Oleh karena itu, mengembangkan kemampuan atribusi yang kuat dan memastikan identifikasi musuh yang akurat sangat penting untuk keberhasilan

[104] Dreyfus, M (2022). *Jumpa Pers 12 November: Joint Standing Operations Against Cyber Criminal Syndicates*. https://ministers.ag.gov.au/media-centre/joint-standing-operation-against-cyber-criminal-syndicates-12-11-2022

operasi siber yang bersifat ofensif. Hal ini dapat dicapai melalui investasi pada teknologi dan metodologi canggih, seperti kecerdasan buatan dan pembelajaran mesin, untuk meningkatkan akurasi dan kecepatan proses atribusi.

Kedua, dari perspektif pertahanan, Australia harus terus mengembangkan dan mengintegrasikan platform intelijen ancaman canggih yang memanfaatkan pembelajaran mesin dan AI untuk mendeteksi dan memprediksi ancaman siber. Platform ini dapat menganalisis data dalam jumlah besar secara real-time, mengidentifikasi pola yang mengindikasikan aktivitas berbahaya, dan memberikan wawasan yang dapat ditindaklanjuti untuk mencegah potensi serangan. Pendekatan proaktif ini akan meningkatkan kemampuan institusi dalam mengantisipasi dan memitigasi ancaman sebelum ancaman tersebut menimbulkan kerugian yang signifikan, sehingga memperkuat kemampuan pertahanan siber secara keseluruhan.

17. Strategi optimalisasi infrastruktur siber.

Karena sifat ancaman siber yang bersifat transnasional dan tanpa batas terhadap keamanan nasional, strategi untuk mengoptimalkan infrastruktur siber harus mempertimbangkan pendekatan internasional dan domestik.

a. Domestik

Analisis dalam bab ini menunjukkan bahwa keamanan siber merupakan tanggung jawab seluruh negara. Semua pemangku kepentingan berisiko terkena serangan siber – mulai dari individu hingga dunia usaha dan pemerintah – dan semuanya mempunyai tanggung jawab untuk berkontribusi dalam memperkuat postur keamanan siber Australia. Namun seperti yang telah dibahas, teori kontrak sosial mengatakan bahwa negaralah yang harus menciptakan dan melindungi kondisi yang menjamin keamanan nasional. Oleh karena itu, meskipun pemerintah tidak dapat bekerja sendirian, harus menjadi pendorong strategi apa pun untuk meningkatkan keamanan siber di tingkat nasional.

Kenyataannya di Australia adalah sektor swasta, bukan pemerintah, yang membangun dan memelihara sebagian besar perangkat keras dan perangkat lunak siber Australia, dan inilah yang dieksploitasi oleh pelaku kejahatan dalam serangan mereka. Oleh karena itu, pemerintah harus bekerja

sama dengan sektor swasta untuk melindungi infrastruktur ini dari ancaman siber. Kemitraan publik-swasta memungkinkan pertukaran intelijen ancaman, praktik terbaik, dan sumber daya antara sektor publik dan swasta. Melalui kolaborasi, pemerintah dan dunia usaha dapat meningkatkan kemampuan kolektif mereka untuk mendeteksi, mencegah, dan merespons insiden siber. ACSC adalah mekanisme utama yang memfasilitasi saran siber dari pemerintah kepada sektor swasta dan individu. ACSC menawarkan berbagai layanan termasuk intelijen ancaman, respons insiden, dan materi pendidikan yang dirancang untuk meningkatkan kesadaran dan pemahaman tentang risiko keamanan siber.

Meskipun ACSC sangat efektif dalam meningkatkan ketahanan dan kesadaran keamanan siber nasional, terdapat potensi untuk lebih memperkuat dan memanfaatkan pengetahuan kolektif pemerintah dan industri untuk mengoptimalkan infrastruktur siber Australia. Untuk mencapai tujuan ini, perlu beralih dari arus informasi satu arah dari pemerintah ke industri, dan menerapkan mekanisme yang memungkinkan terjadinya kolaborasi sejati. Keberhasilan ini memerlukan upaya mengatasi keengganan sektor swasta untuk berbagi informasi mengenai insiden siber dengan pemerintah. Kekhawatiran mengenai kerahasiaan, potensi dampak hukum, dan penyalahgunaan data sensitif menghalangi dunia usaha untuk mengungkapkan pelanggaran siber.[105]

b. Pendekatan berdasarkan analisis

Berdasarkan analisis di atas, disarankan pendekatan strategis berikut:

Pertama, pembagian intelijen ancaman siber secara dua arah antara sektor publik dan swasta harus ditingkatkan. Meskipun sebagian dari intelijen siber pemerintah akan dirahasiakan, langkah-langkah harus diambil untuk memungkinkan dunia usaha yang relevan mengakses informasi ini karena pengungkapannya akan berkontribusi terhadap keamanan nasional. Hal ini dapat dicapai melalui deklasifikasi intelijen yang relevan (kalau cocok) atau dengan memberikan ijin keamanan kepada pejabat siber dalam bisnis yang teridentifikasi dengan ukuran tertentu atau kepentingan nasional. Untuk

[105] Bareja dan Caples, *op.cit.*

membangun kesadaran situasional yang lebih baik dan pemahaman *real-time* mengenai ancaman dan kerentanan, pemerintah harus menetapkan mekanisme hukum yang memberikan kekebalan dari tanggung jawab untuk mendorong sektor swasta agar menyampaikan laporan ancaman dan insiden kepada pemerintah secara tepat waktu. Memberikan jaminan bahwa informasi yang dibagikan tidak akan digunakan untuk penuntutan atau tindakan regulasi lainnya akan meningkatkan kepercayaan bisnis. Pendekatan kolaboratif ini akan memberikan pemahaman yang lebih baik mengenai ancaman yang dihadapi ekosistem keamanan siber nasional guna memfasilitasi pertahanan dan respons yang lebih baik.

Kedua, Dewan Peninjau Insiden Siber (DPIS) harus dibentuk sesegera mungkin untuk memastikan adanya pembelajaran dari insiden siber yang tidak dapat dicegah. DPIS akan memiliki fungsi yang berbeda dengan ACSC, yang difokuskan pada intelijen dan respons ancaman, bukan pada pembelajaran. Memahami insiden siber dan berbagi wawasan dengan para pemangku kepentingan terkait akan memperbaiki postur keamanan siber Australia. DPIS harus berfungsi sebagai entitas independen yang bertugas meninjau insiden siber yang signifikan dan menyebarkan pembelajaran. Untuk memaksimalkan efektivitasnya, DPIS harus terdiri dari perwakilan pemerintah dan industri, memastikan bahwa pengetahuan khusus diterapkan pada tinjauan dan perumusan rekomendasi. Keanggotaan yang luas dari berbagai industri akan mendorong pertukaran informasi lintas sektor dan mendorong solusi inovatif. Proses yang jelas untuk penunjukan DPIS dan pengambilan keputusan harus ditetapkan untuk menjaga integritas dan efektivitas DPIS.

Untuk membangun kemampuan, ketahanan dan kepercayaan, rekomendasi DPIS harus bersifat ‘tidak dapat diatribusikan’ dan fokus pada analisis, dengan tujuan memberikan pembelajaran bagi pemerintah dan dunia usaha. Kegiatan DPIS harus bersifat rahasia dan terfokus pada menghasilkan rekomendasi praktis untuk meningkatkan keamanan siber. Hasil investigasi DPIS – yang dredaksi untuk melindungi privasi sesuai kebutuhan – harus dipublikasikan untuk memastikan pembelajaran disebarluaskan dan berkontribusi pada peningkatan praktik keamanan siber di Australia secara keseluruhan. Yang penting, informasi yang diungkapkan kepada DPIS harus tunduk pada kewajiban kerahasiaan untuk mencegah penggunaannya untuk

tujuan lain. Seperti dijelaskan di atas, jaminan kekebalan dari tanggung jawab kemungkinan besar akan meningkatkan kesediaan dunia usaha untuk bekerja sama dengan kegiatan DPIS.

c. Internasional

Berbeda dengan ancaman keamanan tradisional yang terbatas pada lokasi fisik, ancaman siber dapat berasal dari mana saja di dunia dan menargetkan korban secara global dalam hitungan detik. Informasi yang dikelola oleh jaringan komputer – yang menjalankan utilitas, transportasi, perbankan dan komunikasi – dapat diserang dari lokasi di luar perbatasan Australia.[106] Sifat ancaman yang tidak mengenal batas wilayah ini mempersulit upaya pertahanan, karena para penyerang mengeksploitasi perbedaan dalam undang-undang, peraturan, dan kemampuan penegakan hukum nasional. Penjahat siber dan aktor-aktor yang disponsori negara seringkali beroperasi dari yurisdiksi di mana mereka menghadapi sedikit risiko penuntutan, memanfaatkan sifat global internet untuk melakukan aktivitas mereka dengan impunitas relatif. Keragaman standar teknologi dan pendekatan peraturan di berbagai wilayah dapat menciptakan tantangan dalam menciptakan kerangka kerja keamanan siber global yang kohesif, sehingga penting bagi negara-negara untuk terlibat dalam dialog dan kolaborasi berkelanjutan guna mengatasi ancaman siber bersama secara efektif.

Dari perspektif neoliberalisme, kerja sama siber internasional sangat penting untuk membangun ruang siber global yang stabil dan aman, yang didukung oleh lembaga-lembaga internasional yang efektif dan perjanjian multilateral. Dengan menggunakan sudut pandang teori ini, dapat dipahami bahwa ancaman global seperti keamanan siber memerlukan upaya terkoordinasi dan penciptaan norma dan aturan melalui organisasi internasional seperti PBB dan badan-badan regional. Lembaga-lembaga ini memainkan peran penting dalam memfasilitasi dialog, membangun kepercayaan, dan memastikan kepatuhan terhadap standar dan praktik keamanan siber bersama. Dengan memupuk transparansi, kerja sama, dan

[106] Clarke, R. dan Knake, R. *Cyber War: The Next Threat to National Security and What to Do About it*. Ecco: United States. h.160-1

bantuan timbal balik antar negara, lembaga-lembaga internasional dapat membantu memitigasi ancaman siber, melindungi infrastruktur penting, dan meningkatkan tata kelola internet global. Pendekatan ini tidak hanya memperkuat kemampuan kolektif untuk merespons insiden siber namun juga mendorong supremasi hukum di dunia siber, memastikan bahwa semua negara, terlepas dari posisi global mereka, memiliki suara dalam membentuk tatanan digital global. Oleh karena itu, merupakan kepentingan nasional Australia untuk bekerja sama dengan mitra internasional untuk berbagi intelijen, menyelaraskan undang-undang, dan berkolaborasi dalam penyelidikan dan tindakan penegakan hukum.

Pada tahun 2021, negara-negara anggota PBB menyetujui kerangka kerja untuk perilaku negara yang bertanggung jawab di dunia maya, sehingga kerangka tersebut mengikat secara politis bagi semua negara anggota.[107] Namun, sejarah menunjukkan bahwa kesepakatan mengenai norma-norma secara terpisah tidak akan menjamin kepatuhan terhadap norma-norma tersebut.[108] Dan kerangka kerja yang mengikat secara politik tidak sama dengan undang-undang yang mengikat secara hukum. Jika tidak ada kerangka hukum, maka norma-norma tersebut harus disertai dengan kerangka untuk membangun akuntabilitas dan memberikan konsekuensi jika norma-norma tersebut diabaikan. Hal ini memerlukan kemampuan untuk mengaitkan serangan siber dan kesepakatan mengenai tindakan yang harus dilakukan secara proporsional. Namun, seperti disebutkan sebelumnya, atribusi dapat menjadi sebuah tantangan dan sebagian besar operasi siber yang disponsori negara tidak memenuhi ambang batas *jus contra bellum* (undang-undang yang melarang penggunaan kekuatan antarnegara), sehingga mempersulit upaya untuk melakukan respons.[109]

Bersamaan dengan upaya internasional untuk mengidentifikasi dan menghukum serangan siber berbasis negara, perlu ada peningkatan

---

[107] PBB (2021). *Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final Substantive Report.* A/AC.290/2021/CRP.2

[108] Lewis, J.A. (2022). *Creating Accountability for Global Cyber Norms.* CSIS. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220223_Lewis_Cyber_Norms_Accountability_1.pdf?VersionId=gnbcRAEST2ElGmED3AhM1LOHcNe2TUqd

[109] Delerue, F (2020). *Cyber Operations and International Law*, Cambridge University Press: United Kingrdom. ch.6

kemampuan keamanan siber global. Dari perspektif regional, kemampuan siber suatu negara sangat bervariasi di Asia Tenggara dan Pasifik. Mirip dengan Australia, kawasan ini mengalami peningkatan serangan siber yang menargetkan sektor pemerintah dan swasta. Terdapat negara-negara di kawasan Australia, khususnya di Pasifik, yang memiliki sumber daya terbatas, kesadaran keamanan siber yang tidak memadai, dan kerangka peraturan yang baru, sehingga menjadikan mereka lebih rentan terhadap ancaman siber. Meskipun Australia telah mempunyai program peningkatan kapasitas siber di Asia Tenggara dan Pasifik, yaitu Program Kerja Sama Siber dan Teknologi Kritis, masih banyak yang perlu dilakukan agar kerentanan di kawasan ini tidak menjadi ancaman bagi keamanan nasional Australia.

d. Pendekatan berdasarkan analisis

Berdasarkan analisis di atas, disarankan pendekatan strategis berikut:

Pertama, dalam masalah atribusi, Australia harus bekerja sama dengan negara-negara yang berpikiran sama untuk meningkatkan kepercayaan kolektif untuk mengaitkan serangan siber. Australia telah mengambil langkah awal menuju atribusi kolaboratif, dengan secara terbuka bergabung dengan negara-negara termasuk Inggris dan Amerika Serikat untuk mengeluarkan pernyataan menentang tindakan siber internasional yang jahat.[110] Sebagai bagian dari upaya ini, Australia harus berupaya mengembangkan kemampuan atribusi mitra-mitra regionalnya, dengan mengingat bahwa kemampuan intelijen rahasia tidak selalu diperlukan karena kini terdapat aktor-aktor sektor swasta yang mempunyai kemampuan untuk mengatribusikan sumber tindakan siber yang bermusuhan.[111] Atribusi multilateral kemungkinan besar akan memberikan dampak yang lebih besar dibandingkan dengan masing-masing negara yang bekerja secara terpisah.

Kedua, dalam masalah respons proporsional, Australia harus bekerja sama dengan mitra-mitra yang berpikiran sama dalam kerangka PBB untuk menyepakati dan membangun mekanisme arbitrase dan penuntutan insiden

[110] Lihat misalnya: Wong, *Jumpa Pers 8 Desember - Australian Statement on Russian Cyber Targeting of Democratic Processes*. https://www.foreignminister.gov.au/minister/penny-wong/media-release/australian-statement-russian-cyber-targeting-democratic-processes
[111] Lewis, *op.cit.*

siber. Langkah pertama adalah finalisasi perjanjian internasional mengenai perlawanan terhadap aktivitas siber yang berbahaya. Hal ini akan memberikan kerangka hukum global yang penting yang akan menjadi dasar upaya untuk mengadili pelaku kejahatan siber. Langkah kedua adalah membentuk mekanisme arbitrase, yang mungkin mirip dengan *International Centre for the Settlement of Investment Disputes* (Pusat Internasional untuk Penyelesaian Sengketa Investasi), yang menyediakan tempat independen untuk mendengarkan dan membela tuduhan aktivitas siber dan arbitrase untuk memberikan tanggapan yang tepat.

Ketiga, Australia harus mempertahankan upaya peningkatan kapasitas di kawasan. Namun, mengingat peran penting yang dimainkan sektor swasta dalam upaya keamanan siber global, keterlibatan Australia harus diperluas tidak hanya melalui jalur pemerintah tetapi juga mencakup sektor swasta. Membentuk kelompok kerja keamanan siber regional *1,5 track*, yang mencakup perwakilan pemerintah dan pemangku kepentingan sektor swasta, dapat memfasilitasi penyelarasan dan koordinasi strategi keamanan siber nasional. Kelompok ini harus mendukung penyedia infrastruktur dan industri internasional dalam mengembangkan pendekatan keamanan siber yang kohesif dan lintas yurisdiksi. Australia juga harus menjajaki opsi-opsi untuk mekanisme intelijen dan pembagian ancaman yang lebih matang di kawasan. Misalnya, Australia dapat bermitra dengan *Cybersecurity and Information Centre of Excellence* (Pusat Keunggulan Keamanan Siber dan Informasi) ASEAN untuk mendorong respons di seluruh kawasan terhadap ancaman.

e. Rencana Aksi Strategis

Karena sifat lanskap siber yang berkembang pesat, strategi untuk mengoptimalkan infrastruktur siber Australia harus fokus pada inisiatif jangka pendek dan menengah dengan komitmen terhadap tinjauan dan perubahan secara berkala. Berdasarkan analisis pada uraian Taskap ini, sebuah rencana aksi strategis diusulkan pada Tabel 3. Dalam jangka pendek, rencana aksi difokuskan pada penganggaran, peningkatan kesadaran publik, dukungan bipartisan, kebijakan dan strategi, tata kelola, sumber daya manusia, dan pengembangan kapasitas internasional. Dalam jangka menengah, rencana aksi difokuskan pada investasi dalam teknologi dan inovasi, reformasi legislatif,

penyusunan strategi keamanan nasional, dan pembentukan mekanisme untuk arbitrase internasional dan penuntutan insiden siber. Inisiatif ini akan memerlukan usaha berkelanjutan dan fokus dalam jangka panjang.

Dengan menggunakan kacamata teori kontrak sosial, strategi ini mengasumsikan bahwa pemerintah mempunyai kewajiban mendasar untuk melindungi warga negaranya dan aset-asetnya. Oleh karena itu merupakan tanggung jawab Pemerintah untuk menciptakan ruang siber yang aman. Mennggunakan perspective realisme, strategi ini mengasumsikan sifat anarkis dari sistem internasional dan kepentingan negara yang melekat. Oleh karena itu Pemerintah harus bekerja secara mandiri untuk mengutamakan keamanan nasionalnya. Juga mengacu pada Neoliberalisme, strategi ini mengakui adanya nilai dalam kerja sama. Oleh karena itu, Pemerintah juga harus bekerja sama dengan negara lain, organisasi internasional, dan sektor swasta untuk meningkatkan ketahanan terhadap ancaman siber. Pendekatan ini akan mengoptimalkan infrastruktur siber Australia guna melindungi keamanan nasional Australia.

Tema	Prakarsa	Tindakan	Entitas yang bertanggung jawab	Jangka waktu[112]	Diperkirakan biaya AUD[113]	Ukuran kesuksesan
Anggaran	Mempertahankan tingkat pendanaan siber saat ini.	• Pemerintah harus mempertahankan (sbg minimum) anggaran federal yang saat ini dialokasikan untuk keamanan siber. • Pastikan dana REDSPICE digunakan sepenuhnya dan distribusikan kembali dana yang kemungkinan tidak akan dikeluarkan.	Pemerintah Federal	2025/26	Tidak ada biaya tambahan	Pendanaan untuk inisiatif siber dipertahankan pada tingkat saat ini, atau ditingkatkan, disesuaikan dengan inflasi.

[112] Dinyatakan sebagai tahun keuangan di mana inisiatif akan dimulai. Tahun keuangan Australia dimulai pada bulan Juli dan berakhir pada bulan Juni. Tahun keuangan yang dimulai Juni 2024 dinyatakan sebagai 2024/25.
[113] Perkiraan biaya berdasarkan dokumen anggaran Pemerintah Australia sebelumnya dan informasi lain yang tersedia untuk umum. Proyeksi pengeluaran pemerintah selama empat tahun ke depan setelah tahun keuangan saat ini (2024-25).

Tema	Prakarsa	Tindakan	Entitas yang bertanggung jawab	Jangka waktu[112]	Diperkirakan biaya AUD[113]	Ukuran kesuksesan
Kampanye kesadaran masyarakat	Keterlibatan pemerintah dengan masyarakat mengenai aspek keamanan nasional dari keamanan siber.	• Gunakan peluang media dan keterlibatan publik yang ada. • Kampanye periklanan online yang sederhana dan bertarget.	Departemen Dalam Negeri	2024/25	$8 juta	Interaksi tingkat tinggi dengan konten kampanye – suka, berbagi, dan komentar. Liputan media yang lebih luas mengenai isu-isu siber mencerminkan apresiasi terhadap implikasi keamanan nasional.

Tema	Prakarsa	Tindakan	Entitas yang bertanggung jawab	Jangka waktu[112]	Diperkirakan biaya AUD[113]	Ukuran kesuksesan
Inovasi	Pemerintah akan memfasilitasi inovasi sektor swasta dalam mengembangkan solusi keamanan siber mutakhir yang selaras dengan tujuan keamanan nasional.	• Program kolaborasi siber antara pemerintah, institusi akademis, dan sektor swasta. • Penghargaan inovasi untuk mengakui dan menghargai perusahaan dan individu yang inovatif.	Departemen Dalam Negeri, Departemen Perindustrian, Ilmu Pengetahuan dan Sumber Daya	2025/26	$40 juta	Teknologi baru dikembangkan dan dibawa ke pasar. Ekosistem inovasi dikembangkan dan diperluas, termasuk kemitraan baru dan pusat inovasi.
Peraturan standar keamanan siber	Peraturan beberapa standar sukarela.	• Mengatur standar minimum keamanan siber dan kode praktik.	Departemen Kejaksaan Agung	2025/26	Dalam sumber daya yang ada	Peraturan baru diperkenalkan, yang meningkatkan ketahanan siber dalam dunia usaha.

Tema	Prakarsa	Tindakan	Entitas yang bertanggung jawab	Jangka waktu[112]	Diperkirakan biaya AUD[113]	Ukuran kesuksesan
***Cyber Security Act* (Undang-undang Keamanan Siber)**	Merancang satu undang-undang untuk keamanan siber.	• Konsolidasikan seluruh peraturan perundang-undangan yang ada di bawah satu payung hukum. • Memberikan pedoman yang jelas dan konsisten untuk pelaporan dan respons insiden.	Pemerintah Federal, Departemen Kejaksaan Agung	2026/27	Dalam sumber daya yang ada	Undang-Undang Keamanan Siber baru diperkenalkan untuk menyederhanakan kepatuhan terhadap peraturan.

Tema	Prakarsa	Tindakan	Entitas yang bertanggung jawab	Jangka waktu[112]	Diperkirakan biaya AUD[113]	Ukuran kesuksesan
Dukungan bipartisan	Pemerintah harus mengambil langkah-langkah untuk mendapatkan dukungan bipartisan untuk pendekatan bersama terhadap keamanan siber.	• Melibatkan perwakilan dari partai politik besar dalam konsultasi mengenai kebijakan atau undang-undang baru. • Membentuk komite bipartisan untuk mengawasi pengembangan dan implementasi kebijakan dan strategi keamanan siber.	Pemerintah Federal	2024/25	Dalam sumber daya yang ada	Kedua belah pihak di parlemen secara konsisten mendukung inisiatif siber dan alokasi sumber daya, terlepas dari siapa yang membentuk pemerintahan pada saat itu.

Tema	Prakarsa	Tindakan	Entitas yang bertanggung jawab	Jangka waktu[112]	Diperkirakan biaya AUD[113]	Ukuran kesuksesan
Strategi Keamanan Nasional	Peluncuran Strategi Keamanan Nasional.	• Pengembangan Strategi Keamanan Nasional melalui proses keseluruhan pemerintahan yang menempatkan ancaman siber dalam konteks keamanan nasional yang lebih luas.	Departemen Perdana Menteri dan Kabinet	2026/27	$15 juta	Perhatian dan sumber daya yang sesuai dialokasikan untuk inisiatif siber.

Tema	Prakarsa	Tindakan	Entitas yang bertanggung jawab	Jangka waktu[112]	Diperkirakan biaya AUD[113]	Ukuran kesuksesan
Pemantauan dan evaluasi strategi	Memperjelas bagaimana implementasi Strategi Keamanan Siber Australia (ACSS) akan dikomunikasikan.	• Tetapkan metrik pelaporan yang jelas. • Komunikasikan jadwal pelaporan publik.	Kantor Keamanan Siber Nasional	2024/25	Dalam sumber daya yang ada	Pemerintah memberikan pembaruan rutin mengenai implementasi strategi termasuk keberhasilan dan kegagalannya. Pendekatan strategis disesuaikan.
Siklus Strategi Keamanan Siber (ACSS) Dua Tahunan	ACSS baru diterbitkan setiap dua tahun sekali.	• ACSS dikaji dan disesuaikan dalam siklus dua tahunan.	Kantor Keamanan Siber Nasional	2025/26	$10 juta	Strategi siber Australia tetap gesit dan selalu mengikuti perkembangan lingkungan ancaman yang berubah dengan cepat.

Tema	Prakarsa	Tindakan	Entitas yang bertanggung jawab	Jangka waktu[112]	Diperkirakan biaya AUD[113]	Ukuran kesuksesan
Koordinator Siber	Koordinator Siber menjadi posisi yang ditunjuk dengan wewenang yang lebih lengkap.	• Proses perekrutan yang kompetitif, dengan pelamar yang berhasil ditunjuk berdasarkan kontrak jangka waktu tetap. • Kekuatan penegakan untuk Koordinator yang akan ditingkatkan.	Pemerintah Federal	2024/25	$4 juta	Perekrutan Koordinator Siber selesai pada akhir penugasan militer saat ini. Wewenang untuk menegakkan kepatuhan terhadap peraturan dan standar keamanan siber berarti lembaga pemerintah dan operator infrastruktur penting harus lebih cermat dalam menerapkan standar keamanan mereka.

Tema	Prakarsa	Tindakan	Entitas yang bertanggung jawab	Jangka waktu[112]	Diperkirakan biaya AUD[113]	Ukuran kesuksesan
Kantor Keamanan Siber Nasional (KKSN)	KKSN diubah menjadi kantor pemerintahan secara keseluruhan.	• Petugas senior yang tepat dari masing-masing lembaga dengan tanggung jawab dunia maya untuk diintegrasikan ke dalam KKSN.	Koordinator Siber	2024/25	Dalam sumber daya yang ada	Berbagi informasi yang lebih baik antar departemen, pengambilan keputusan yang lebih efisien, dan respons yang terkoordinasi terhadap ancaman siber.

Tema	Prakarsa	Tindakan	Entitas yang bertanggung jawab	Jangka waktu[112]	Diperkirakan biaya AUD[113]	Ukuran kesuksesan
Keberagaman tenaga kerja siber	Rekrutmen tenaga kerja yang lebih beragam.	• Penjangkauan dan kemitraan yang ditargetkan dengan lembaga pendidikan, organisasi profesi dan kelompok masyarakat. • Penyediaan program beasiswa, magang dan mentoring yg tepat sasaran. • Mempromosikan budaya inklusivitas dengan kebijakan keberagaman dan inklusi yang kuat.	Industri	2024/25	Tidak ada biaya bagi pemerintah (dipimpin oleh industri)	Peningkatan jumlah perempuan dan kelompok minoritas lainnya yang bekerja di bidang keamanan siber, menghasilkan lebih banyak tenaga kerja siber.

Tema	Prakarsa	Tindakan	Entitas yang bertanggung jawab	Jangka waktu[112]	Diperkirakan biaya AUD[113]	Ukuran kesuksesan
Peningkatan keterampilan siber	Kemitraan antara industri dan akademisi untuk memberikan peningkatan keterampilan bagi tenaga kerja siber.	• Program pelatihan dan lokakarya bersama. • Pembentukan sertifikasi keterampilan khusus sektor.	Industri	2024/25	Tidak ada biaya bagi pemerintah (dipimpin oleh industri)	Keterampilan tenaga kerja siber Australia tetap *up to date* dengan gambaran ancaman saat ini.
Otomatisasi	AI akan dimanfaatkan untuk meringankan krisis tenaga kerja.	• Alat berbasis AI diperkenalkan untuk mengotomatiskan tugas-tugas rutin seperti deteksi ancaman dan respons insiden.	Industri	2025/26	Tidak ada biaya bagi pemerintah (dipimpin oleh industri)	Para profesional keamanan siber dapat fokus pada aktivitas keamanan siber yang lebih kompleks dan strategis, sehingga menghasilkan postur keamanan siber yang lebih baik.

Tema	Prakarsa	Tindakan	Entitas yang bertanggung jawab	Jangka waktu[112]	Diperkirakan biaya AUD[113]	Ukuran kesuksesan
Investasi dalam teknologi	Investasi dalam teknologi canggih untuk menyerang dan bertahan	• AI dan pembelajaran mesin untuk meningkatkan akurasi dan kecepatan atribusi. • Memanfaatkan data besar untuk mendeteksi, memprediksi, dan memitigasi ancaman siber.	ASD	2027/28	$30 juta	Australia mampu menghubungkan serangan siber dengan lebih akurat. Australia telah meningkatkan kemampuan ofensifnya, berkontribusi terhadap upaya global untuk menghentikan pelaku siber sebelum mereka menyerang. Australia telah meningkatkan kemampuan pertahanannya.

Tema	Prakarsa	Tindakan	Entitas yang bertanggung jawab	Jangka waktu[112]	Diperkirakan biaya AUD[113]	Ukuran kesuksesan
Atribusi internasional	Bekerja dengan mitra internasional untuk meningkatkan atribusi.	• Mengembangkan kemampuan atribusi mitra regional. • Bekerja sama secara multilateral untuk secara publik mengaitkan serangan siber global.	Departemen Luar Negeri dan Perdagangan	2025/26	$6 juta	Terdapat peningkatan jumlah serangan siber yang secara terbuka dikaitkan dengan aktor negara atau non-negara. Atribusi ini seringkali bersifat multilateral.

Tema	Prakarsa	Tindakan	Entitas yang bertanggung jawab	Jangka waktu[112]	Diperkirakan biaya AUD[113]	Ukuran kesuksesan
Respon proporsional	Bekerja dengan mitra internasional untuk membangun mekanisme arbitrase dan penuntutan insiden siber.	• Kerja sama untuk menyelesaikan perjanjian internasional tentang melawan aktivitas siber yang berbahaya. • Kerjasama untuk membentuk mekanisme arbitrase siber internasional.	Departemen Luar Negeri dan Perdagangan	2026/27	$3 juta	Jumlah serangan yang disponsori negara dan negara berkurang karena para pelaku ini dicegah untuk terlibat dalam aktivitas siber yang berbahaya.

Tema	Prakarsa	Tindakan	Entitas yang bertanggung jawab	Jangka waktu[112]	Diperkirakan biaya AUD[113]	Ukuran kesuksesan
Pembangunan kemampuan	Program peningkatan kemampuan dipertahankan dan diperluas hingga mencakup sektor swasta	• Membentuk kelompok kerja keamanan siber regional *1,5 Track*. • Bermitra dengan pusat berbagi informasi regional untuk meningkatkan intelijen siber dan berbagi ancaman.	Departemen Luar Negeri dan Perdagangan	2025/26	$4,5 juta	Kawasan ini meningkatkan ketahanan sibernya, yang ditandai dengan pertahanan siber yang lebih baik dan pemulihan yang lebih cepat dari serangan siber.

Tabel 3: Rencana Aksi Strategis

BAB IV
PENUTUP

18. Kesimpulan

Berdasarkan analisis dalam taskap ini mengenai optimalisasi infrastruktur siber untuk melindungi keamanan nasional Australia, maka dengan mengacu pada setiap pertanyaan kajian, dapat disimpulkan sebagai berikut:

a. Membangun infrastruktur siber yang mendukung keamanan nasional mendukung juga kemakmuran dan ketahanan Australia. Seiring dengan semakin banyaknya aktor negara dan non-negara yang mengembangkan kemampuan siber tingkat lanjut, risiko aktivitas siber sangat berbahaya bagi kepentingan Australia meningkat. Hal ini tidak hanya mengancam negara dari perspektif keamanan tradisional, namun juga individu dan masyarakat dari perspektif keamanan manusia.

b. Regulasi berperan penting dalam membangun dan mempertahankan infrastruktur siber yang kuat. Kebijakan harus jelas menetapkan standar dan tanggung jawab untuk melindungi sistem informasi dan data. Regulasi memastikan semua pihak memahami peran mereka dalam menjaga keamanan siber, memudahkan penerapan langkah-langkah efektif, dan menegakkan kepatuhan. Dengan kerangka regulasi yang kuat dan adaptif, infrastruktur siber mampu menghadapi ancaman saat ini dan masa depan, melindungi keamanan nasional, dan mendorong stabilitas ekonomi.

c. Infrastruktur siber mempunyai dampak yang signifikan terhadap keamanan nasional di era digital ini. Infrastruktur ini berperan dalam mendukung dan mengamankan seluruh aspek kehidupan Australia. Keamanan siber merupakan tantangan yang beragam dan kompleks yang mencakup dimensi ekonomi, sosial, politik, dan strategis. Kompleksitas ancaman siber memerlukan pendekatan holistik terhadap infrastruktur siber yang menggabungkan dimensi peraturan,

prosedur, dan kebijakan untuk memastikan keamanan nasional yang kuat dan tangguh.

d. Mengoptimalkan infrastruktur siber guna melindungi keamanan nasional memerlukan strategi yang terintegrasi dan kolaboratif. Strategi yang diusulkan dalam Taskap ini didasarkan pada teori realisme, neoliberalisme, dan kontrak sosial yang menempatkan pemerintah sebagai pihak yang bertanggung jawab atas keamanan siber Australia. Pemerintah harus menjamin keamanan siber tersebut melalui tindakan yang baik independen maupun kooperatif guna mengoptimalkan infrastruktur siber dan melindungi keamanan nasional Australia. Pendekatan dalam Taskap ini akan memastikan kerangka keamanan siber yang tangguh dan adaptif, mampu menahan tantangan dunia digital yang semakin kompleks dan berkembang pesat.

19. Rekomendasi

Merujuk pada strategi optimalisasi infrastruktur siber dalam rangka melindungi keamanan nasional Australia, penulis merekomendasikan tindakan berikut:

a. Untuk mengoptimalkan infrastruktur siber Australia guna mendukung keamanan nasional, pemerintah federal (di tingkat politik) harus mempertahankan tingkat pendanaan siber dan mendapatkan dukungan bipartisan untuk pendekatannya terhadap keamanan siber. Pemerintah federal (dipimpin oleh Menteri Keamanan Siber) juga harus mengambil langkah-langkah untuk meningkatkan tata kelola siber antar departemen terkait. Langkah pertama untuk mencapai hal ini adalah dengan meningkatkan wewenang Koordinator Siber dan merestrukturisasi *National Cyber Security Office* (Kantor Keamanan Siber Nasional) untuk mengintegrasikan perwakilan dari seluruh departemen terkait.

b. Untuk memperkuat undang-undang dan peraturan siber di Australia, pemerintah federal (dipimpin oleh Departemen Kejaksaan Agung) harus menyusun *Cyber Security Act* untuk menyatukan undang-

undang dan peraturan terkait ke dalam satu undang-undang pusat. Sebagai bagian dari proses tersebut, standar minimum keamanan siber dan kode praktik harus diamanatkan.

c. Untuk memastikan pendekatan holistik terhadap keamanan siber, pemerintah federal (dipimpin oleh Departemen Luar Negeri dan Perdagangan dan Department Dalam Negeri, kerja sama dengan Departemen Perindustrian, Ilmu Pengetahuan dan Sumber Daya) harus terus bekerja sama dengan dunia bisnis dan mitra internasional. Kerja sama tersebut harus focus pada peningkatan kapasitas serta inovasi dan pemanfaatan teknologi baru. Teknologi-teknologi tersebut tidak hanya dapat dimanfaatkan untuk meringankan kekurangan tenaga kerja siber dalam negeri, namun juga dapat meningkatkan kecepatan dan akurasi dalam mengidentifikasi serangan siber di Australia dan kawasan sekitarnya.

d. Untuk mengelola ancaman siber yang berkembang pesat, pemerintah federal (dipimpin oleh Departemen Dalam Negeri dan Departemen Perdana Menteri dan Kabinet) harus mengambil pendekatan tangkas untuk mengoptimalkan infrastruktur siber. Strategi siber baru harus dikeluarkan setiap dua tahun dan harus dilengkapi dengan strategi keamanan nasional. Untuk memastikan akuntabilitas dan transparansi, pemerintah harus memberikan informasi terkini secara berkala kepada masyarakat mengenai implementasi strategi sibernya.

Dengan mengadopsi pendekatan dalam Taskap ini diharapkan infrastruktur siber dapat dioptimalisasi guna melindungi keamanan nasional Australia.

DAFTAR PUSTAKA

Buku

Clarke, R dan Knake, R (2010). *Cyberwar: The Next Threat to National Security and What to do About it*. Ecco: United States.

Delerue, F. (2020). *Cyber Operations and International Law*. Cambridge University Press: United Kingdom

Dunne, T. Kurki, M. dan Smith, S. (2020). *International Relations Theories: Discipline and Diversity* (edisi 5). Oxford University Press: United Kingdom

IGI Global (2022). *Research Anthology on Business Aspects of Cybersecurity*. Information Resources Management Association: Pennsylvania.

Lopez-Claros dkk (2020). *Global Governance and the Emergence of Global Institutions for the 21st Century*. Cambridge University Press: United Kingdom

Tay, K.L. (2023). *ASEAN Cyber-security Cooperation: Towards a Regional Emergency-response Framework*. The International Institute for Strategic Studies: United Kingdom

Williams, M.C. (2009). *The Realist Tradition and the Limits of International Relations*. Cambridge University Press: United Kingdom

Peraturan Perundang-undangan

Commonwealth of Australia, *Crimes Act 1914*

Commonwealth of Australia, *Privacy Act 1988*

Commonwealth of Australia, *Criminal Code Act 1995*

Commonwealth of Australia, *Corporations Act 2001*

Commonwealth of Australia, *Security of Critical Infrastucture Act 2018*

Commonwealth of Australia, *Telecommunications Sector Security Reforms 2019*

Commonwealth of Australia, *Online Safety Act 2021*

Dokumen

ACSC (2024). Information Security Manual (Maret). https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism diakses pada Jumat 31 Mei 2024 pukul 1515 WIB.

Al Jazeera (2023). *US, Japan, South Korea Step Up Efforts to Counter North Korea Cyber-Threats.* https://www.aljazeera.com/news/2023/12/9/us-japan-south-korea-launch-new-efforts-to-counter-n-korea-cyber-threats diakses pada Sabtu 11 Mei 2024, pukul 1000 WIB.

Australian Signals Directorate (2021). *ASD Cyber Threat Report 2020-21*. https://www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Annual%20Cyber%20Threat%20Report%20-%202020-2021.pdf diakses pada Sabtu 17 Februari 2024, pukul 1310 WIB.

Australian Signals Directorate (2022). *ASD Cyber Threat Report 2021-22*. https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf diakses pada Sabtu 17 Februari 2024, pukul 1305 WIB.

Australian Signals Directorate (2023). *ASD Cyber Threat Report 2022-23*. https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf diakses pada Sabtu 17 Februari 2024, pukul 1300 WIB.

Australian Signal's Directorate, *REDSPICE: A Blueprint for Growing ASD's Capabilities.* *https://www.asd.gov.au/sites/default/files/2022-05/ASD-REDSPICE-Blueprint.pdf* diakses pada Minggu 18 Februari 2024, pukul 0800 WIB.

Australian Communications and Media Authority (2023). *Communications and Media in Australia: How We Use the Internet.* https://www.acma.gov.au/publications/2023-12/report/communications-and-media-australia-how-we-use-internet diakses pada Kamis 11 April 2024, pukul 1730.

Blackberry (2023). *Global Threat Intelligence Report, August Edition.* https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/bbcomv4/blackberry-com/en/solutions/threat-intelligence/2023/ laporan-ancaman-intelijen-agustus/Blackberry-Global-Ancaman-Laporan-Intelijen-Agustus-2023.pdf diakses pada Sabtu 17 Februari 2024, pukul 1330 WIB.

Commonwealth of Australia (2020). *Australia's Cyber Security Strategy 2020.* Department of Home Affairs and Trade: Canberra.

Commonwealth of Australia (2023). *Australian Cyber Security Strategy 2023-2030*. Department of Home Affairs: Canberra.

Commonwealth of Australia (2024). *Budget Papers 2023-24*. https://archive.budget.gov.au/2023-24/index.htm diakses pada Selasa 26 Juni 2024 pukul 1830 WIB.

Commonwealth of Australia (2000). *Defence White Paper 2000.* Department of Defence: Canberra.

Commonwealth of Australia (2009). *Defence White Paper 2009*. Department of Defence: Canberra.

Commonwealth of Australia (2016). *Defence White Paper 2016*. Department of Defence: Canberra.

Commonwealth of Australia (2020). *Defence Strategic Update*. Department of Defence: Canberra.

Commonwealth of Australia (2024). *National Defence Strategy*. Department of Defence: Canberra.

Commonwealth of Australia (2012). *National Security Strategy*. Department of Prime Minister and Cabinet: Canberra

Department of Home Affairs *Protective Security Policy Framework* https://www.protectivesecurity.gov.au/about diakses pada Jumat 31 Mei 2024 pukul 1530 WIB.

International Telecommunications Union (2020). *Global Cyber Security Index 2020*. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx diakses pada Sabtu 15 Maret, pukul 1000 WIB.

Neaher, G. dkk (2021). *Standardizing the Future: How Can the United States Navigate the Geopolitics of International Technology Standards?* https://www.atlanticcouncil.org/in-depth-research-reports/report/standardizing-the-future-how-can-the-united-states-navigate-the-geopolitics-of-international-technology-standards/ diakses pada Jumat 31 Mei 2024 pukul 1400 WIB.

Neelam, R. (2023). *Lowy Institute Poll 2023 Report*. https://poll.lowyinstitute.org/report/2023/ diakses pada Minggu 30 Maret 2024 pukul 1100 WIB.

PBB (2021). *Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final Substantive Report.* A/AC.290/2021/CRP.2

Program Pembangunan PBB (UNDP) (1994). *Human Development Report 1994*. Oxford University Press: New York

Singapore Government (2021). *The Singapore Cybersecurity Strategy*. Cyber Security Agency of Singapore: Singapore.

Jurnal/Artikel

Bareja, M. dan Caples, A. (2023). *Australia's New Cybersecurity Strategy Tackles the Tough Issues*. Australian Strategic Policy Institute https://www.aspistrategist.org.au/australias-new-cybersecurity-strategy-tackles-the-tough-issues/ diakses pada Jumat 21 Juni 2024 pukul 1400.

Burnyeat, G. dan Johansson, M.S. (2022). 'An Anthropology of the Social Contract: The Political Power of an Idea.' *Critique of Anthropology* Vol 42(3).

Feakin, T. dkk (2016). *Agenda for Change 2016: Cybersecurity*. *Australian Strategic Policy Institute*. https://www.aspistrategist.org.au/agenda-change-cybersecurity/ diakses pada Rabu 1 Mei 2024 pukul 1815 WIB.

Fell, J. (2024). 'Medibank hacker linked to Russian hacking syndict REvil' *ABC News* https://www.abc.net.au/news/2024-01-24/medibank-hacker-linked-to-russian-hacking-syndicate-revil/103381342 diakses pada Rabu 29 Mei 2024 pukul 1615 WIB.

Lewis, J.A. (2022). *Creating Accountability for Global Cyber Norms*. CSIS. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220223_Lewis_Cyber_Norms_Accountability_1.pdf?VersionId=gnbcRAEST2ElGmED3AhM1LOHcNe2TUgd diakses pada Jumat 21 Juni 2024 pukul 1500.

Mao, F. (2023). *Vanuatu: Hackers Strand Pacific Island Government for Over a Week*. BBC News, 18 November https://www.bbc.com/news/world-asia-63632129 diaskses pada Selasa 2 April 2024 pukul 1700 WIB.

Mueller, G.B. dkk (2023), *Cyber Operations During the Russo-Ukrainian War*. CSIS https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war diaskses pada Rabu 27 Maret 2024 pukul 2000 WIB.

Muslain, L. (2023). *As Cybercrime Evolves, Organisational Resilience Demands a Mindset Shift*, Australian Strategic Policy Institute. https://www.aspistrategist.org.au/as-cybercrime-evolves-organisational-resilience-demands-a-mindset-shift/ diakses pada Rabu 27 Maret pukul 2030 WIB.

Seekbek, L. (2023). *The Choice of Cyber Coordinator Reflects Weakened Cyber Capability*. Strategic Analysis Australia. https://strategicanalysis.org/the-choice-of-cyber-coordinator-reflects-weakened-cyber-capability/ diakses pada Sabtu 22 Juni 2024 pukul 1300 WIB.

Shah, R. (2023). *Getting Regulation Right: Approaches to Improving Australia's Cyber Security*, Australian Strategic Policy Institute https://aspi.org.au/report/getting-regulation-right-approaches-improving-australias-cybersecurity diakses pada Jumat 31 Mei 0935 WIB.

Stewart, C. (2010). 'What is Cyberinfrastructure', *Proceedings of SIGUCCS 2010* (Norfolk, VA 24-27 October)

Uren, D. (2023). *Australian Ports in a Cyber Storm*, Australian Strategic Policy Institute, https://www.aspistrategist.org.au/australian-ports-in-a-cyber-storm/ diakses pada Rabu 27 Maret pukul 2015 WIB.

Website/Internet

Antunes, S. dan Camisao, I. (2018). *Introducing Realism in International Relations Theory*. https://www.e-ir.info/2018/02/27/introducing-realism-in-international-relations-theory/#google_vignette diakses pada Sabtu 23 Maret 2024 pukul 0900 WIB.

AustCyber (2024). *AustCyber Report Reveals Local Cyber Security Sector is at a Pivotal Juncture as Global Copetitiveness Slips and the Skills Gap Widens.*

https://www.austcyber.com/sites/default/files/2024-05/SCP%20media%20release%20%282%29.pdf diakses pada Sabtu 22 Juni 2024 pukul 1030 WIB.

Austech Media (2023), *Women Critical to Future of Australia's Cyber Security Workforce*. https://www.techbusinessnews.com.au/news/women-critical-to-future-of-australias-cyber-security-workforce/#google_vignette diakses pada Sabtu 22 Juni 2024 pukul 1200 WIB.

Australian Information Security Association (2024). *Australian Federal Government's 2024-25 Budget* https://www.aisa.org.au/Public/Public/News_and_Media/News/2024/Australian-Federal-Government-s-2024-25-Budget.aspx diakses pada Jumat 5 April 2024 pukul 1600 WIB.

Australian Signals Directorate. *Australian Cyber Security Centre Glossary*. https://cyber.gov.au/glossary/threat-actor diakses pada Minggu 18 Februari 2024, pukul 0815 WIB.

Brangwin, N. (2013). *Cyber Security*, Parliament of Australia. https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/pubs/BriefingBook44p/Cyber#:~:text=In%20November%202009%2C%20the%20Cyber,CERT%20Australia)%20and%20the%%2020CSOC diakses pada Rabu 1 Mei 2024, pukul 1800 WIB.

Britannica (2024). *Social Contract*. https://www.britannica.com/topic/social-contract diakses pada Minggu 7 April 2024, pukul 0900 WIB.

CSIS (2024). *Significant Cyber Incidents*. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents diakses pada Rabu 26 Juni 2024 1945 WIB.

Cyber and Infrastructure Security Centre. *Security of Critical Infrastructure Act 2018*. https://www.cisc.gov.au/legislation-regulation-and-compliance/soci-act-2018 diaskses pada Minggu 7 April 2024 pukul 1030 WIB.

Department of Home Affairs, *Cyber Coordinator*, https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/cyber-coordinator diakses pada Minggu 7 April 2024 pukul 1100.

e-Governance Academy Foundation, *National Cyber Security Index.* https://ncsi.ega.ee/ncsi-index/?order=rank&type=c diakses pada Senin 15 April 2024 pukul 1000 WIB.

IBM (2022). *What is Cyber Action?* https://www.ibm.com/topics/cyber-action diakses pada Mingggu 14 April 2024 pukul 1305 WIB.

IBM (2022). *What is Cybersecurity?* https://www.ibm.com/topics/cybersecurity diakses pada Mingggu 14 April 2024 pukul 1300 WIB.

IBM (2022). *What is Ransomware?* https://www.ibm.com/topics/ransomware diakses pada Kamis 27 Juni 2024 pukul 1800 WIB.

ISC2 (2023). *ISC2 Reveals Growth in Global Cybersecurity Workforce, But Record-Breaking Gap of 4 Million Cybersecurity Professionals Looms.* https://www.isc2.org/Insights/2023/10/ISC2-Reveals-Workforce-Growth-But-Record-Breaking-Gap-4-Million-Cybersecurity-Professionals diakses pada Sabtu 22 Juni 2024 pukul 1015 WIB.

Korab-Karpowicz (2023). 'Political Realism in International Relations', *Stanford Encyclopedia of Philosophy*. https://plato.stanford.edu/entries/realism-intl-relations/ diakses pada Senin 14 Mei 2024 pukul 1230 WIB.

Macpherson, J dkk (2023). *Australia's Cyber Strategy – A Bold Regulatory Reform Agenda.* https://www.ashurst.com/en/insights/australias-cyber-strategy-a-bold-regulatory-reform-agenda/ diakses pada Sabtu 22 Juni 2024 pukul 1830.

Merriam-Webster. *Optimization*. https://www.merriam-webster.com/dictionary/optimization diakses pada Jumat 16 Februari pukul 1600 WIB.

National Institute of Standards and Technology. *Cyber Threat.* https://csrc.nist.gov/glossary/term/Cyber_Threat diakses pada Mingggu 14 April 2024 pukul 1310 WIB.

National Institute of Standards and Technology. *NIST Computer Security Resource Centre*. https://csrc.nist.gov/glossary/term/attack_surface#:~:text=attack%20surface%20Definitions%3A%20The%20set%20of%20points%20on,data%20from%

2C%20that%20system%2C%20system%20element%2C%20or%20environment. diakses pada Minggu 18 Februari 2024, pukul 0800 WIB.

National Institute of Standards and Technology (2022), *NIST Updates Cybersecurity Guidance for Supply Chain Risk Management*. https://www.nist.gov/news-events/news/2022/05/nist-updates-cybersecurity-guidance-supply-chain-risk-management diakses pada Senin 21 Mei 2024 pukul 1100 WIB.

Parliament of Australia (2021). *Australian Government Expenditure.* https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/BudgetReview202021/AustralianGovernmentExpenditure diakses pada Kamis 16 Mei 2024 pukul 1900.

Webber Insurance Services (2024). *The Complete List of Data Breaches in Australia for 2018-2024* https://www.webberinsurance.com.au/data-breaches-list#twentyfour diakses pada Senin 15 April 2024 pukul 0900 WIB.

World Economic Forum (2024). *2023 Was a Big Year For Cybercrime – Here's How We Can Make Our Systems Safer.* https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety/ diakses pada Senin 15 April 2024 pukul 0845 WIB.

World Economic Forum (2023). *Why is the Asia Pacific Region A Target for Cybercrime – and What Can be Done About it?* https://www.weforum.org/agenda/2023/06/asia-pacific-region-the-new-ground-zero-cybercrime/ diakses pada Senin 15 April 2024 pukul 0915 WIB.

Lain-lain

Dreyfus, M. (2022). *Jumpa Pers 12 November: Joint Standing Operations Against Cyber Criminal Syndicates*. https://ministers.ag.gov.au/media-centre/joint-standing-operation-against-cyber-criminal-syndicates-12-11-2022 diakses pada Senin 17 Juni 2024 pukul 1300 WIB.

Medcalf, R. (2022). *The 2022 Order of Australia Lecture* (pidato, Australian National University, 7 Desember). https://www.anu.edu.au/news/all-news/making-sense-of-national-security diaskes pada Senin 15 April 2024 pukul 0930 WIB.

Noble, R. (2021). *ASD: 75 Years and Ready for Tomorrow* (pidato, National Press Club, 18 November) https://www.asd.gov.au/news-events-speeches/speeches/director-general-asd-speech-national-press-club diakses pada Rabu 29 Mei 2024 1530 WIB.

O'Neil, C (2023). *Joint Press Conference with the Assistant Minister for Foreign Affairs*. https://ministers.dfat.gov.au/minister/tim-watts/transcript/joint-press-conference-minister-home-affairs-and-cyber-security diakses pada Rabu 29 Mei 2024 pukul 1600 WIB.

O'Neil, C. (2023). *Jumpa Pers 22 November*. https://minister.homeaffairs.gov.au/ClareONeil/Pages/Press-conference-22112023.aspx diakses pada Rabu 29 Mei 2024 pukul 1545 WIB.

Prime Minister of Australia dan Minister for Home Affairs *Jumpa Pers 23 Juni: Appointment of National Cyber Security Coordinator*. https://www.pm.gov.au/media/appointment-national-cyber-security-coordinator diakses pada Jumat 10 Mei 2024 pukul 1300 WIB.

Wong, P. (2023). *Jumpa Pers 8 Desember: Australian Statement on Russian Cyber Targeting of Democratic Processes*. https://www.foreignminister.gov.au/minister/penny-wong/media-release/australian-statement-russian-cyber-targeting-democratic-processes diakses pada Rabu 29 Meti 2024 pukul 1600 WIB.

Lampiran 1: Alur Pikir

OPTIMALISASI INFRASTRUKTUR SIBER GUNA MELINDUNGI KEAMANAN NASIONAL AUSTRALIA

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

DAFTAR RIWAYAT HIDUP

NAMA: Jessica Kerr

PANGKAT: -

TEMPAT LAHIR: Sydney, Australia

TANGGAL LAHIR: 23 Juli 1986

ALAMAT: Pakubuwono Menteng, Jl. K.H. Wahid Hasyim No.110-112, Kb. Sirih, Kec. Menteng, Kota Jakarta Pusat, DKI Jakarta, 10340.

PENDIDIKAN

S1, *Bachelor of International Studies*, University of New South Wales, 2008

S2, *Master of Arts (Strategy & Security)*, UNSW@ADFA, 2016

JABATAN

2023-2024, *Direktur Strategi*, Departement Pertahanan

2020-2023, *Direktur Asia Tenggara*, Departement Pertahanan

2018-2020, *Asisten Direktur Hubungan Internasional*, Departement Pertahanan

2014-2018, *Asisten Direktur Indonesia*, Departement Pertahanan

2011-2014, *Petugas Kebijakan Asia Utara*, Departement Pertahanan

2010-2011, *Petugas Kebijakan Papua Nugini*, Departement Pertahanan

2009, *Peserta Program Pengembangan Pascasarjana*, Departement Pertahanan