EDITOR:
ASEP IWA SOEMANTRI
HERU PRASETYO

PELUANG & KENDALA
CYBERPOLITIK
INDONESIA EMAS 2045

TIM PENULIS:
BUDI PRAMONO
LUKMAN YUDHO PRAKOSO
IVAN YULIVAN

PELUANG & KENDALA
CYBERPOLITIK
INDONESIA EMAS 2045

TIM PENULIS:
BUDI PRAMONO
LUKMAN YUDHO PRAKOSO
IVAN YULIVAN

Penerbit Widina

PELUANG & KENDALA CYBERPOLITIK INDONESIA EMAS 2045

Penulis:
Budi Pramono
Lukman Yudho Prakoso
Ivan Yulivan

Desain Cover:
Septian Maulana

Sumber Ilustrasi:
www.freepik.com

Tata Letak:
Handarini Rohana

Editor:
Asep Iwa Soemantri
Heru Prasetyo

ISBN:
978-623-500-190-6
978-623-500-191-3 (PDF)

Cetakan Pertama:
Mei, 2024

PENERBIT:
WIDINA MEDIA UTAMA
Komplek Puri Melia Asri Blok C3 No. 17 Desa Bojong Emas
Kec. Solokan Jeruk Kabupaten Bandung, Provinsi Jawa Barat

Anggota IKAPI No. 360/JBA/2020
Website: www.penerbitwidina.com
Instagram: @penerbitwidina
Telepon (022) 87355370

KATA PENGANTAR

Selamat datang dalam perjalanan intelektual yang menantang ini, yang bertujuan untuk menyelami kawasan yang semakin kompleks dan krusial dalam dunia modern: cyberpolitik. Dalam era di mana teknologi digital merajai hampir setiap aspek kehidupan, penting bagi kita untuk memahami betapa pentingnya peran cyberpolitik dalam membentuk masa depan bangsa kita.

Buku ini berfokus pada Indonesia Emas 2045, sebuah visi ambisius yang menuntut inovasi, ketangguhan, dan kesiapan dalam menghadapi tantangan yang belum pernah terjadi sebelumnya. Melalui lensa cyberpolitik, kami mengeksplorasi peluang dan kendala yang muncul dalam mencapai visi besar ini.

Karya ini tidak hanya ditujukan untuk kalangan akademisi, tetapi juga untuk pembuat kebijakan, praktisi teknologi, dan semua individu yang tertarik dalam memahami dinamika kompleks yang berkembang di dunia maya. Dengan menyelami berbagai perspektif dan pemikiran yang terkemuka dalam bidang ini, kami berharap pembaca akan mendapatkan pemahaman yang lebih dalam tentang bagaimana teknologi informasi dan komunikasi dapat membentuk arah masa depan bangsa kita.

Kami ingin menyampaikan apresiasi yang tulus kepada semua penulis, pakar, dan kontributor yang telah berbagi wawasan dan pengetahuan mereka dalam pembuatan buku ini. Tanpa kolaborasi mereka, karya ini tidak akan mungkin terwujud.

Akhirnya, kami berharap bahwa buku ini dapat menjadi sumber inspirasi dan panduan yang berharga bagi mereka yang berusaha membangun Indonesia menuju masa depan yang gemilang. Mari kita bersama-sama menjawab tantangan cyberpolitik dengan kepala tegak, semangat pantang menyerah, dan tekad untuk meraih Indonesia Emas 2045.

Penulis

Mayor Jenderal TNI Dr. Budi Pramono, S.I.P., M.M., M.A., (GSC)., CIQaR., CIQnR., M.O.S., M.C.E., CIMMR.

DAFTAR ISI

BAB 1
DINAMIKA LINGKUNGAN STRATEGIS

Dinamika lingkungan strategis merujuk pada perubahan dan interaksi kompleks antara berbagai faktor politik, ekonomi, sosial, dan militer di tingkat global, regional, dan lokal. Ini mencakup berbagai aspek yang memengaruhi kebijakan dan strategi negara-negara, organisasi internasional, dan aktor non-negara dalam menjalankan kepentingan dan tujuan mereka. Beberapa elemen utama dalam dinamika lingkungan strategis termasuk:

a. Kekuatan Ekonomi: Persaingan ekonomi antara negara-negara besar, pertumbuhan ekonomi regional, dan dinamika perdagangan internasional memainkan peran penting dalam menentukan posisi dan pengaruh suatu negara di arena global.
b. Kekuatan Militer: Kemajuan teknologi militer, penyebaran senjata nuklir, dan dinamika keamanan regional menjadi faktor utama dalam membentuk hubungan kekuasaan antara negara-negara.
c. Diplomasi dan Hubungan Internasional: Perubahan dalam struktur aliansi, kemitraan strategis, dan diplomasi antarnegara memengaruhi dinamika geopolitik dan kekuasaan global.
d. Perubahan Demografi: Pertumbuhan populasi, migrasi massal, dan perubahan demografis lainnya memengaruhi kebijakan domestik dan lanskap geopolitik regional.
e. Perubahan Lingkungan dan Sumber Daya: Perubahan iklim, keberlanjutan lingkungan, dan persaingan atas sumber daya alam menjadi faktor yang semakin penting dalam menentukan kebijakan dan strategi negara-negara.
f. Teknologi dan Inovasi: Kemajuan dalam teknologi informasi, kecerdasan buatan, dan teknologi lainnya memengaruhi cara negara-negara berkomunikasi, berperang, dan bekerja sama di tingkat internasional.
g. Isu-isu Keamanan Non-Tradisional: Terorisme, kejahatan transnasional, dan keamanan siber menjadi ancaman yang semakin kompleks dan memengaruhi dinamika lingkungan strategis.

Dengan memahami dinamika lingkungan strategis ini, negara-negara dan aktor-aktor internasional dapat merencanakan kebijakan yang lebih efektif dan responsif terhadap tantangan dan peluang yang ada di dunia saat ini.

DAFTAR PUSTAKA

Kissinger, Henry. (2014). "World Order: Reflections on the Character of Nations and the Course of History." Pengantar yang komprehensif tentang dinamika politik global dari masa lalu hingga saat ini, menyoroti peran kekuatan besar, konflik, dan kerja sama internasional.

Friedman, George. (2009). "The Next 100 Years: A Forecast for the 21st Century." Memberikan gambaran tentang tren-tren strategis yang mungkin mempengaruhi dunia dalam abad ke-21, termasuk pergeseran kekuatan geopolitik dan teknologi.

Mahbubani, Kishore. (2008). "The New Asian Hemisphere: The Irresistible Shift of Global Power to the East." Menjelaskan pergeseran kekuatan geopolitik dari Barat ke Timur, dengan fokus pada dinamika politik dan ekonomi di Asia.

Zakaria, Fareed. (2008). "The Post-American World." Menganalisis konsekuensi dari penurunan kekuatan relatif Amerika Serikat dan munculnya kekuatan-kekuatan lain dalam politik global.

Buzan, Barry, dan Hansen, Lene. (2009). "The Evolution of International Security Studies." Memberikan pemahaman mendalam tentang perkembangan teori-teori keamanan internasional dari masa lalu hingga saat ini, termasuk pergeseran dalam fokus studi.

Huntington, Samuel. (1996). "The Clash of Civilizations and the Remaking of World Order." Menyoroti pentingnya identitas budaya dalam menentukan konflik dan kerja sama di tingkat internasional.

Fukuyama, Francis. (2012). "The Origins of Political Order: From Prehuman Times to the French Revolution." Menyajikan analisis tentang bagaimana institusi politik berkembang dari masa lalu hingga masa kini, mempengaruhi dinamika lingkungan strategis.

Kissinger, Henry. (2018). "World Order: Reflections on the Character of Nations and the Course of History." Lanjutan dari karyanya sebelumnya, membahas dinamika lingkungan strategis yang mempengaruhi tatanan global saat ini.

BAB 2
ANALISIS ANCAMAN

Analisis ancaman adalah proses sistematis untuk mengidentifikasi, mengevaluasi, dan memahami ancaman potensial yang mungkin dihadapi oleh suatu entitas, seperti negara, organisasi, atau individu. Tujuan dari analisis ancaman adalah untuk membantu entitas tersebut dalam merencanakan dan mengimplementasikan langkah-langkah yang efektif dalam menghadapi risiko dan mengurangi dampak negatif yang dapat timbul dari ancaman tersebut. Berikut adalah langkah-langkah utama dalam melakukan analisis ancaman.

A. IDENTIFIKASI ANCAMAN

Langkah pertama dalam analisis ancaman adalah mengidentifikasi semua ancaman potensial yang mungkin dihadapi. Ancaman dapat berasal dari berbagai sumber, termasuk negara asing, kelompok bersenjata, terorisme, kejahatan organisasi, atau bencana alam.

Identifikasi ancaman merupakan langkah penting dalam kegiatan analisis ancaman yang melibatkan proses sistematis untuk mengidentifikasi berbagai jenis ancaman yang mungkin dihadapi oleh suatu entitas, seperti negara, organisasi, atau individu. Berikut adalah beberapa langkah umum yang dilakukan dalam identifikasi ancaman:

Pengumpulan Informasi: Langkah pertama dalam identifikasi ancaman adalah mengumpulkan informasi yang relevan tentang lingkungan strategis di mana entitas tersebut beroperasi. Ini melibatkan analisis tren global, dinamika regional, dan perkembangan lokal yang dapat memengaruhi keamanan dan kepentingan entitas.

Analisis Intelijen: Menggunakan data dan informasi yang dikumpulkan, tim analisis intelijen melakukan analisis mendalam untuk mengidentifikasi potensi ancaman yang mungkin timbul. Ini melibatkan evaluasi berbagai faktor seperti niat, kapabilitas, dan kesempatan dari aktor yang berpotensi menjadi ancaman.

Pemodelan Ancaman: Setelah identifikasi awal, tim analisis dapat menggunakan teknik pemodelan untuk memperkirakan jenis-jenis ancaman yang mungkin terjadi di masa depan. Ini dapat melibatkan pemodelan skenario yang berbeda berdasarkan perkiraan perubahan lingkungan strategis dan perilaku aktor-aktor terkait.

DAFTAR PUSTAKA

Roberts, Brad. (2009). "Terrorism and Global Security: The Nuclear Threat." Buku ini menyajikan analisis tentang ancaman terorisme global, dengan fokus khusus pada ancaman nuklir dan implikasinya terhadap keamanan global.

Walt, Stephen M. (2018). "The Hell of Good Intentions: America's Foreign Policy Elite and the Decline of U.S. Primacy." Memberikan analisis tentang berbagai ancaman terhadap keamanan nasional Amerika Serikat, termasuk ancaman tradisional dan baru.

Johnston, Alastair Iain. (2003). "Social States: China in International Institutions, 1980-2000." Menyajikan studi tentang bagaimana China menghadapi berbagai ancaman dan memanfaatkan institusi internasional untuk melindungi kepentingannya.

Buzan, Barry, et al. (1998). "Security: A New Framework for Analysis." Buku ini memberikan kerangka analisis yang komprehensif tentang keamanan, termasuk berbagai jenis ancaman dan cara-cara untuk mengatasi mereka.

Mearsheimer, John J. (2001). "The Tragedy of Great Power Politics." Menyajikan analisis tentang ancaman yang dihadapi oleh kekuatan besar dalam sistem internasional, dan bagaimana mereka merespons ancaman tersebut.

Deudney, Daniel, dan Ikenberry, G. John. (2009). "The Myth of the Autocratic Revival: Why Liberal Democracy Will Prevail." Menganalisis berbagai ancaman terhadap sistem liberal internasional dan argumen tentang mengapa demokrasi liberal akan tetap kuat.

Allison, Graham. (2017). "Destined for War: Can America and China Escape Thucydides's Trap?" Menyajikan analisis tentang ancaman yang timbul dari persaingan kekuatan besar, khususnya antara Amerika Serikat dan Tiongkok, dan upaya untuk menghindari konflik.

Gray, Colin S. (1999). "Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History." Menyajikan analisis tentang berbagai ancaman terhadap keamanan nasional, termasuk ancaman militer dan non-militer, serta strategi untuk menghadapinya

BAB 3
INDONESIA EMAS 2045

"Indonesia Emas 2045" adalah visi yang ditetapkan oleh pemerintah Indonesia untuk mencapai status sebagai negara maju dan kuat secara ekonomi, politik, dan sosial pada tahun 2045, yang merupakan peringatan 100 tahun kemerdekaan Indonesia. Visi ini mencakup berbagai aspek pembangunan nasional, termasuk pertumbuhan ekonomi, kesejahteraan sosial, keamanan, dan keberlanjutan lingkungan.

Beberapa poin penting dalam Indonesia Emas 2045 termasuk:

A. PERTUMBUHAN EKONOMI BERKELANJUTAN

Indonesia bertujuan untuk menjadi salah satu ekonomi terbesar di dunia pada tahun 2045 dengan pertumbuhan ekonomi yang berkelanjutan dan inklusif. Langkah-langkah strategis diperlukan untuk meningkatkan investasi, produktivitas, dan daya saing industri nasional.

Untuk mencapai pertumbuhan ekonomi yang berkelanjutan menuju visi Indonesia Emas 2045, beberapa langkah strategis perlu dipertimbangkan:

1. **Pembangunan Infrastruktur**: Investasi besar dalam pembangunan infrastruktur menjadi kunci. Infrastruktur yang baik, seperti jaringan transportasi, energi, telekomunikasi, dan pendukung lainnya, akan menciptakan lingkungan yang kondusif untuk pertumbuhan ekonomi yang berkelanjutan.
2. **Penguatan Sektor Industri**: Diversifikasi dan penguatan sektor industri menjadi penting. Selain sektor tradisional seperti pertanian, perikanan, dan manufaktur, fokus pada industri kreatif, teknologi, dan layanan juga diperlukan untuk meningkatkan daya saing ekonomi.
3. **Peningkatan Kualitas Sumber Daya Manusia**: Investasi dalam pendidikan, pelatihan keterampilan, dan peningkatan kualitas sumber daya manusia akan meningkatkan produktivitas tenaga kerja dan inovasi. Hal ini akan membantu menciptakan ekonomi yang berbasis pengetahuan dan teknologi.
4. **Peningkatan Investasi dan Inovasi**: Mendorong investasi swasta dan mempromosikan inovasi dalam berbagai sektor ekonomi akan memberikan dorongan bagi pertumbuhan ekonomi yang berkelanjutan. Insentif, deregulasi, dan lingkungan bisnis yang kondusif perlu diperhatikan.

DAFTAR PUSTAKA

Kementerian Perencanaan Pembangunan Nasional/Bappenas. (2018). "Visi Indonesia 2045: Indonesia Maju dan Berdaulat, Terwujudnya Indonesia Emas 2045."

Masyarakat Ekonomi Syariah Indonesia (MESI). (2020). "Indonesia Emas 2045: Menggagas Masyarakat Ekonomi Syariah."

Forum Indonesia Maju. (2021). "Rencana Pembangunan Jangka Menengah Nasional 2020-2024: Menuju Indonesia Maju dan Lestari."

Badan Perencanaan Pembangunan Nasional (Bappenas). (2019). "Perencanaan Pembangunan Jangka Menengah Nasional 2020-2024: Akselerasi Pembangunan Menuju Indonesia Maju."

Kementerian Perindustrian Republik Indonesia. (2020). "Making Indonesia 4.0: Menuju Era Revolusi Industri 4.0 dan Indonesia Emas 2045."

Pusat Penelitian Kebijakan dan Strategi Pembangunan, Kementerian PPN/Bappenas. (2020). "Pendekatan Sains, Teknologi, dan Inovasi dalam Meraih Indonesia Emas 2045."

Kementerian Pariwisata dan Ekonomi Kreatif Republik Indonesia. (2019). "Strategi Nasional Pariwisata Indonesia 2019-2024: Indonesia sebagai Destinasi Utama Dunia Menuju Indonesia Emas 2045."

Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia. (2019). "Strategi Nasional Riset dan Inovasi 2019-2045: Merajut Indonesia Emas 2045 Melalui Riset dan Inovasi."

BAB 4
PELUANG CYBERPOLITIK

Peluang dalam ranah cyberpolitik dapat menjadi pendorong kemajuan dan inovasi dalam berbagai aspek kehidupan, termasuk ekonomi, keamanan, dan kesejahteraan sosial. Berikut adalah beberapa peluang yang dapat dimanfaatkan dalam cyberpolitik:

A. PERTUMBUHAN EKONOMI DIGITAL

Kemajuan teknologi informasi dan komunikasi telah menciptakan peluang besar dalam ekonomi digital. Pemerintah dapat mengambil langkah-langkah untuk mendukung pertumbuhan sektor ini melalui kebijakan yang mendorong investasi, inovasi, dan pengembangan infrastruktur teknologi.

Pertumbuhan ekonomi digital menjadi salah satu peluang utama yang muncul dari bidang cyberpolitik. Berikut adalah gambaran tentang bagaimana pertumbuhan ekonomi digital menjadi peluang dalam konteks cyberpolitik:

1. **Peningkatan Aksesibilitas dan Koneksi**: Melalui cyberpolitik yang mempromosikan akses internet yang luas dan terjangkau, lebih banyak orang dapat terhubung ke internet. Ini membuka pintu bagi pertumbuhan ekonomi digital dengan meningkatkan basis pelanggan potensial untuk produk dan layanan digital.
2. **Pembangunan Ekosistem Startup**: Kebijakan yang mendukung inovasi dan kewirausahaan di bidang teknologi informasi dan komunikasi (TIK) mendorong perkembangan ekosistem startup. Startup digital muncul dengan solusi baru dan inovatif dalam berbagai sektor, termasuk e-commerce, layanan keuangan digital, teknologi kesehatan, dan banyak lagi.
3. **Perluasan Pasar Digital**: Melalui platform perdagangan elektronik dan aplikasi mobile, perusahaan dapat memperluas jangkauan pasar mereka secara signifikan. Ini memungkinkan bisnis untuk menjangkau konsumen di lokasi yang jauh tanpa batasan geografis yang signifikan.
4. **Peningkatan Efisiensi Bisnis**: Penggunaan teknologi informasi dan komunikasi dalam proses bisnis dapat meningkatkan efisiensi operasional dan mengurangi biaya. Ini termasuk otomatisasi proses bisnis, manajemen rantai pasokan yang terintegrasi, dan penggunaan analitik data untuk pengambilan keputusan yang lebih baik.

DAFTAR PUSTAKA

Arquilla, John, dan Ronfeldt, David. (Eds.). (1997). "In Athena's Camp: Preparing for Conflict in the Information Age." Santa Monica, CA: Rand Corporation.

Libicki, Martin C. (2009). "Cyberdeterrence and Cyberwar." Santa Monica, CA: Rand Corporation.

Rid, Thomas. (2013). "Cyber War Will Not Take Place." Oxford University Press.

Singer, P. W., dan Friedman, A. (2014). "Cybersecurity and Cyberwar: What Everyone Needs to Know." Oxford University Press.

Clarke, Richard A., dan Knake, Robert K. (2010). "Cyber War: The Next Threat to National Security and What to Do About It." HarperCollins.

Carr, Jeffrey. (2012). "Inside Cyber Warfare: Mapping the Cyber Underworld." O'Reilly Media.

Brenner, Joel. (2010). "America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare." Penguin Books.

Clarke, Richard A., dan Knake, Robert K. (2012). "Cyber War: The Next Threat to National Security." Ecco.

Goodman, Seymour E., dan Lin, Herbert S. (2014). "The Battle for Cyber Supremacy: China, America, and the Struggle for Technological Dominance." Routledge.

Schneier, Bruce. (2015). "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World." W. W. Norton & Company.

BAB 5
KENDALA CYBERPOLITIK

Kendala dalam ranah cyberpolitik dapat menghambat pembangunan dan pemanfaatan teknologi informasi dan komunikasi (TIK) secara efektif, serta menghadirkan tantangan dalam mengelola risiko yang terkait dengan penggunaan teknologi digital. Berikut adalah beberapa kendala yang sering dihadapi dalam cyberpolitik:

A. KEAMANAN SIBER

Ancaman siber seperti serangan malware, peretasan data, dan serangan DDoS (*Distributed Denial of Service*) merupakan kendala utama dalam cyberpolitik. Perlindungan infrastruktur digital dan data menjadi prioritas untuk mencegah kerugian dan kebocoran informasi yang merugikan.

Kendala dalam bidang keamanan siber merupakan tantangan utama yang dihadapi dalam cyberpolitik. Berikut adalah penjelasan lebih lanjut mengenai kendala-kendala tersebut:

1. **Serangan Malware**: Malware merupakan perangkat lunak berbahaya yang dirancang untuk merusak, mengganggu, atau mencuri informasi dari sistem komputer. Serangan malware dapat menyebabkan kerusakan sistem, kehilangan data sensitif, dan gangguan operasional yang serius bagi organisasi atau individu. Kendala ini menuntut penerapan kebijakan yang efektif dalam perlindungan sistem dan jaringan dari serangan malware yang merugikan.
2. **Peretasan Data**: Peretasan data atau pencurian data adalah ancaman yang serius bagi keamanan cyber. Pelaku peretasan dapat mencuri informasi rahasia, data pribadi, atau rahasia industri yang sensitif. Peretasan data dapat mengakibatkan kerugian finansial, reputasi yang rusak, dan dampak yang merugikan bagi individu, perusahaan, atau bahkan negara. Oleh karena itu, kebijakan cyberpolitik harus berfokus pada perlindungan data sensitif dan penerapan tindakan keamanan yang kuat untuk mencegah peretasan data.
3. **Serangan DDoS (*Distributed Denial of Service*)**: Serangan DDoS bertujuan untuk mengganggu ketersediaan layanan online dengan membanjiri target dengan lalu lintas internet yang tidak sah. Hal ini dapat menyebabkan situs web atau layanan online menjadi tidak dapat diakses oleh pengguna yang sah, menyebabkan gangguan operasional dan kerugian finansial bagi organisasi yang menjadi target. Kebijakan

DAFTAR PUSTAKA

Nye, Joseph S. Jr. (2010). "Cyber Power." Harvard Kennedy School.

Clarke, Richard A., dan Knake, Robert K. (2012). "Cyber War: The Next Threat to National Security." Ecco.

Brenner, Joel. (2010). "America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare." Penguin Books.

Singer, P. W., dan Friedman, A. (2014). "Cybersecurity and Cyberwar: What Everyone Needs to Know." Oxford University Press.

Libicki, Martin C. (2009). "Cyberdeterrence and Cyberwar." Santa Monica, CA: Rand Corporation.

Rid, Thomas. (2013). "Cyber War Will Not Take Place." Oxford University Press.

Schneier, Bruce. (2015). "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World." W. W. Norton & Company.

Carr, Jeffrey. (2012). "Inside Cyber Warfare: Mapping the Cyber Underworld." O'Reilly Media.

Goodman, Seymour E., dan Lin, Herbert S. (2014). "The Battle for Cyber Supremacy: China, America, and the Struggle for Technological Dominance." Routledge.

Clarke, Richard A., dan Knake, Robert K. (2010). "Cyber War: The Next Threat to National Security and What to Do About It." HarperCollins.

BAB 6
STRATEGI CYBERPOLITIK INDONESIA EMAS 2045

Untuk mencapai visi Indonesia Emas 2045 dalam ranah cyberpolitik, Indonesia perlu menerapkan strategi yang komprehensif dan berkelanjutan. Berikut adalah beberapa strategi yang dapat membantu mencapai tujuan tersebut:

A. PENGUATAN KEAMANAN SIBER

Membangun pertahanan siber yang kuat adalah kunci dalam melindungi infrastruktur digital dan data negara dari serangan siber. Ini meliputi peningkatan kemampuan deteksi dan respons terhadap ancaman siber, pembangunan sistem keamanan yang tangguh, dan kerjasama dengan lembaga internasional untuk pertukaran informasi dan penegakan hukum.

Untuk merumuskan strategi penguatan keamanan siber dalam mendukung visi Indonesia Emas 2045, kita dapat menerapkan konsep teori Clausewitz yang meliputi *Ends* (tujuan), *Ways* (cara), dan *Means* (sarana). Berikut adalah gambaran tentang bagaimana strategi tersebut dapat dirumuskan:

1. **_Ends_ (Tujuan)**:
   - Tujuan akhir dari strategi penguatan keamanan siber adalah untuk menciptakan lingkungan digital yang aman, tangguh, dan dapat diandalkan untuk mendukung pertumbuhan ekonomi dan kesejahteraan masyarakat Indonesia pada tahun 2045.
   - Tujuan jangka panjangnya adalah untuk mengurangi risiko dan kerentanan terhadap serangan cyber, melindungi infrastruktur kritis, data sensitif, dan informasi penting dari ancaman cyber.

2. **_Ways_ (Cara)**:
   - Melakukan pembangunan kapasitas dalam bidang keamanan siber dengan meningkatkan keterampilan dan pengetahuan para profesional keamanan siber melalui program pelatihan dan sertifikasi yang komprehensif.
   - Menerapkan kebijakan dan regulasi yang ketat untuk melindungi infrastruktur kritis, data pribadi, dan informasi rahasia dari serangan

DAFTAR PUSTAKA

Arquilla, John, dan Ronfeldt, David. (Eds.). (1997). "In Athena's Camp: Preparing for Conflict in the Information Age." Santa Monica, CA: Rand Corporation.

Arquilla, John, dan Ronfeldt, David. (Eds.). (1997). "In Athena's Camp: Preparing for Conflict in the Information Age." Santa Monica, CA: Rand Corporation. Buku ini membahas persiapan konflik dalam era informasi, meskipun tidak secara khusus berkaitan dengan teori Clausewitz, tetapi dapat memberikan wawasan tentang strategi dalam ranah cyber.

Buzan, Barry, et al. (1998). "Security: A New Framework for Analysis." Menyajikan kerangka analisis tentang keamanan, termasuk potensi penerapan teori Clausewitz dalam konteks keamanan modern.

Carr, Jeffrey. (2012). "Inside Cyber Warfare: Mapping the Cyber Underworld." O'Reilly Media.

Clarke, Richard A., dan Knake, Robert K. (2010). "Cyber War: The Next Threat to National Security and What to Do About It." HarperCollins.

Clarke, Richard A., dan Knake, Robert K. (2012). "Cyber War: The Next Threat to National Security." Ecco.

Clarke, Richard A., dan Knake, Robert K. (2012). "Cyber War: The Next Threat to National Security." Ecco. Buku ini membahas ancaman perang siber terhadap keamanan nasional, namun lebih berfokus pada aspek praktis dan kebijakan daripada aspek teoritis.

Libicki, Martin C. (2009). "Cyberdeterrence and Cyberwar." Santa Monica, CA: Rand Corporation.

Libicki, Martin C. (2009). "Cyberdeterrence and Cyberwar." Santa Monica, CA: Rand Corporation. Buku ini membahas konsep deterrance dan perang siber, meskipun tidak secara khusus menggunakan teori Clausewitz.

Rid, Thomas. (2013). "Cyber War Will Not Take Place." Oxford University Press.

Rid, Thomas. (2013). "Cyber War Will Not Take Place." Oxford University Press. Buku ini mengeksplorasi pertanyaan fundamental tentang perang siber dan konflik di era digital, dan meskipun tidak secara langsung menggunakan teori Clausewitz, beberapa konsep yang mungkin terkait dengan teori tersebut dibahas.

Schneier, Bruce. (2015). "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World." W. W. Norton & Company.

BAB 7
CYBERPOLITIK DI NEGARA LAIN

Cyberpolitik adalah konsep yang mengacu pada penggunaan teknologi digital dan internet dalam arena politik dan pemerintahan. Dengan semakin terhubungnya dunia melalui jaringan digital, negara-negara di berbagai belahan dunia menghadapi tantangan dan peluang baru dalam hal keamanan siber, propaganda digital, serta partisipasi politik online. Pengantar ini akan mengeksplorasi bagaimana cyberpolitik berkembang di beberapa kawasan utama dunia, termasuk Eropa, Asia, Afrika, dan Amerika.

A. CYBERPOLITIK DI EROPA

1. **Keamanan Siber dan Kebijakan Digital:**
   - Di Eropa, Uni Eropa (UE) memainkan peran penting dalam mengoordinasikan kebijakan keamanan siber di antara negara anggotanya. Inisiatif seperti "EU Cybersecurity Act" dan pembentukan "*European Union Agency for Cybersecurity* (ENISA)" bertujuan untuk memperkuat keamanan siber di seluruh benua.
   - Negara-negara seperti Jerman dan Prancis sangat aktif dalam mengembangkan kebijakan keamanan siber dan infrastruktur digital untuk melindungi data nasional dan perusahaan-perusahaan penting dari ancaman siber.

2. **Propaganda dan Disinformasi:**
   - Eropa juga menghadapi tantangan besar terkait propaganda dan disinformasi digital, terutama menjelang pemilihan umum. Negara-negara seperti Estonia, yang sering menjadi target serangan siber, telah mengambil langkah-langkah proaktif dalam meningkatkan literasi digital dan pertahanan siber.

Implementasi cyberpolitik di negara-negara Eropa seperti Prancis, Inggris, Jerman, Belgia, dan Belanda melibatkan berbagai kebijakan, strategi, dan kasus-kasus terkenal yang menunjukkan betapa pentingnya keamanan siber, perlindungan data, dan regulasi digital di era modern. Berikut adalah penjelasan tentang implementasi cyberpolitik di masing-masing negara beserta beberapa kasus yang menonjol:

DAFTAR PUSTAKA

Agence nationale de la sécurité des systèmes d'information (ANSSI)**. (n.d.). Retrieved from [ssi.gouv.fr](https://www.ssi.gouv.fr/)

CSIS**. (2021). **Significant Cyber Incidents**. Retrieved from [csis.org](https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents)

Cyber Security Strategy for Germany 2016**. (2016). Retrieved from [bmi.bund.de](https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2016/cyber-security-strategy-for-germany-2016.pdf)

Cybersecurity and Infrastructure Security Agency (CISA)**. (n.d.). Retrieved from [cisa.gov](https://www.cisa.gov/)

Cyberspace Administration of China (CAC)**. (n.d.). Retrieved from [cac.gov.cn](http://www.cac.gov.cn/)

Digital Trust Center**. (n.d.). Retrieved from [digitaltrustcenter.nl](https://www.digitaltrustcenter.nl/)

Federal Information Security Modernization Act (FISMA)**. (2014). Retrieved from [congress.gov](https://www.congress.gov/bill/113th-congress/house-bill/1163)

Federal Office for Information Security (BSI)**. (n.d.). Retrieved from [bsi.bund.de](https://www.bsi.bund.de/EN/Home/home_node.html)

French National Cybersecurity Strategy**. (2015). Retrieved from [ssi.gouv.fr](https://www.ssi.gouv.fr/uploads/IMG/pdf/Strategie_nationale_de_securite_du_numerique_EN.pdf)

Ghana's National Cyber Security Policy & Strategy**. (2019). Retrieved from cybersecurity.gov.gh

Government Communications Headquarters (GCHQ)**. (n.d.). Retrieved from [gchq.gov.uk](https://www.gchq.gov.uk/)

Japan's Cybersecurity Strategy**. (2021). Retrieved from [nisc.go.jp](https://www.nisc.go.jp/eng/pdf/cybersecuritystrategy-en.pdf)

Korea Internet & Security Agency (KISA)**. (n.d.). Retrieved from [kisa.or.kr](https://www.kisa.or.kr/eng/main.jsp)

Mandiant**. (2013). **APT1: Exposing One of China's Cyber Espionage Units**. Retrieved from [fireeye.com](https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf)

Mueller, R. S.** (2019). **Report on the Investigation into Russian Interference in the 2016 Presidential Election**. Retrieved from [justice.gov](https://www.justice.gov/storage/report.pdf)

National Cyber Security Centre (NCSC) Netherlands**. (n.d.). Retrieved from [ncsc.nl](https://english.ncsc.nl/)

National Cyber Security Centre (NCSC)**. (n.d.). Retrieved from [ncsc.gov.uk](https://www.ncsc.gov.uk/)

National Cyber Security Policy of India**. (2013). Retrieved from [meity.gov.in](https://www.meity.gov.in/writereaddata/files/National%20Cyber%20Security%20Policy%20%281%29.pdf)

National Cyber Security Strategy 2016-2021**. (2016). Retrieved from [gov.uk](https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021)

National Cyber Security Strategy 2018**. (2018). Retrieved from [nationaalcoordinatorterrorismebestrijding.nl](https://www.nctv.nl/onderwerpen/cybersecurity/nationaal-cybersecurity-beleid)

National Cyber Strategy of the United States of America**. (2018). Retrieved from [whitehouse.gov](https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf)

National Cybersecurity Strategy for Kenya**. (2014). Retrieved from [ict.go.ke](https://www.ict.go.ke/wp-content/uploads/2020/01/NATIONAL-CYBERSECURITY-STRATEGY.pdf)

Nigeria's National Cybersecurity Policy and Strategy**. (2014). Retrieved from [cert.gov.ng](https://cert.gov.ng/ngcert/resources/National%20Cybersecurity%20Policy%20&%20Strategy.pdf)

South Africa National Cybersecurity Policy Framework**. (2012). Retrieved from [gov.za](https://www.gov.za/documents/national-cybersecurity-policy-framework-south-africa)

Symantec**. (2017). **The WannaCry Ransomware Attack**. Retrieved from [symantec.com](https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wannacry-ransomware-attack)

U.S. Cyber Command (USCYBERCOM)**. (n.d.). Retrieved from [cybercom.mil](https://www.cybercom.mil/)

U.S. Department of Justice**. (2018). **Operation Wire Wire: International Business Email Compromise Takedown**. Retrieved from [justice.gov](https://www.justice.gov/opa/pr/operation-wire-wire-international-business-email-compromise-takedown)

BAB 8
IMPLEMENTASI CYBERPOLITIK PADA PILPRES INDONESIA 2024

A. DAMPAK NEGATIF

Cyberpolitik, penggunaan teknologi digital dan siber dalam proses politik, telah menjadi bagian integral dari pemilu di seluruh dunia, termasuk Pilpres Indonesia 2024. Meskipun teknologi digital membawa banyak manfaat, ada beberapa dampak negatif yang telah muncul selama dan setelah proses Pilpres. Berikut adalah penjelasan beberapa dampak negatif yang signifikan:

1. **Keamanan Siber dan Serangan Digital**
   - **Kejadian:** Pilpres 2024 di Indonesia telah menghadapi berbagai serangan siber, termasuk peretasan situs web KPU, upaya pembajakan data pemilih, dan serangan DDoS yang mengganggu akses ke informasi penting.
   - **Dampak:**
     - **Gangguan Proses Pemilu:** Serangan ini mengganggu penghitungan suara, distribusi informasi, dan operasi logistik pemilu.
     - **Kepercayaan Publik:** Insiden ini mengurangi kepercayaan masyarakat terhadap integritas dan keamanan proses pemilu.

2. **Disinformasi dan Kampanye Hitam**
   - **Kejadian:** Media sosial dipenuhi dengan disinformasi, berita palsu, dan kampanye hitam yang menargetkan kandidat tertentu.
   - **Dampak:**
     - **Polarisasi Politik:** Penyebaran informasi yang salah memecah belah masyarakat, memperdalam perpecahan politik, dan menciptakan ketidakpercayaan antara berbagai kelompok pemilih.
     - **Pemilih Terpengaruh:** Banyak pemilih terpengaruh oleh informasi palsu, yang mempengaruhi keputusan mereka di kotak suara dan menciptakan bias yang tidak sehat dalam proses pemilu.

DAFTAR PUSTAKA

Badan Siber dan Sandi Negara. (https://www.bssn.go.id)

Centre for Strategic and International Studies. (2019). "Cyberpolitik di Indonesia: Tantangan dan Peluang dalam Menanggapi Ancaman Siber." Jakarta: CSIS Indonesia.

Firmansyah, H., & Widodo, A. (2018). "Cyberpolitik dalam Pemilu Legislatif di Era Digital." Jurnal Kajian Politik, 3(1), 78-92.

Institute for Policy Analysis of Conflict. (2021). "Cyberpolitik dan Radikalisasi Online di Indonesia: Peran Teknologi Digital dalam Penyebaran Ekstremisme." Jakarta: IPAC.

Jurnal Ilmu Politik dan Pemerintahan, 7(2), 112-125. Diakses dari [link](https://jurnal.uns.ac.id/jip/vol7/iss2/7).

Kementerian Komunikasi dan Informatika Republik Indonesia. (https://www.kominfo.go.id)

Nurmandi, A. (Ed.). (2019). "Teknologi Informasi dan Komunikasi dalam Pemilu di Indonesia: Perspektif Cyberpolitik." Yogyakarta: Penerbit Gava Media.

Pratama, R. (2022). "Peran Media Sosial dalam Kontestasi Politik: Studi Kasus Cyberpolitik di Pemilu Indonesia." Jurnal Media Komunikasi Politik, 8(1), 45-58. Diakses dari [link](https://www.jmkp.or.id/index.php/jmkp/article/view/64).

Rachman, B., & Santoso, D. (2021). "Dampak Kampanye Digital dalam Pemilu: Tinjauan dari Perspektif Cyberpolitik."

Susanto, H., & Nugraha, P. (2020). "Cyberpolitik: Tantangan dan Prospek Pemilu Digital di Indonesia." Jakarta: Penerbit Buku Kompas.

Wibowo, A., & Indrayana, B. (2020). "Analisis Cyberpolitik dalam Kontestasi Pemilu Indonesia 2019." Jurnal Politik Muda, 4(2), 123-140.

PELUANG & KENDALA
CYBERPOLITIK
INDONESIA EMAS 2045

Buku ini merupakan sebuah karya yang merangkum kompleksitas dinamika lingkungan strategis dalam konteks cyberpolitik yang menghadirkan tantangan dan peluang bagi Indonesia menuju visi besar, yaitu Indonesia Emas 2045. Dengan fokus pada aspek teknologi digital dan politik cyber, buku ini disusun sebagai referensi akademik yang relevan bagi berbagai kalangan yang tertarik dan membutuhkan pemahaman mendalam mengenai isu-isu ini.

Melalui analisis ancaman dan peluang yang komprehensif, buku ini membantu pembaca untuk memahami peran krusial teknologi informasi dan komunikasi dalam pembangunan bangsa. Penulis menguraikan berbagai strategi yang dapat diterapkan untuk menyambut tantangan-tantangan tersebut dengan penuh kesiapan dan inovasi.

Dengan memadukan berbagai perspektif ahli dan pemikir terkemuka dalam bidang cyberpolitik, buku ini tidak hanya memberikan gambaran tentang lanskap saat ini, tetapi juga menawarkan wawasan tentang arah masa depan Indonesia dalam era digital. Buku ini bukan hanya sekadar panduan, tetapi juga menjadi pangkal diskusi dan inspirasi bagi para pembuat kebijakan, praktisi teknologi, akademisi, dan masyarakat umum yang tertarik untuk berkontribusi dalam mencapai visi Indonesia.

Penerbit widina
www.penerbitwidina.com

ISBN 978-623-500-190-6
9 786235 001906