ORATIO directa

Vol. 3, No. 1, (2021) - pp. 15-18
10.59017/oratiodirecta.v3i1.58

ANCAMAN PERANG SIBER DI ERA DIGITAL DAN SOLUSI KEAMANAN NASIONAL INDONESIA

Cyberwarfare Threats in the Digital Era and Solutions for Indonesia's National Security

Salomon A.M. Babys

Program Studi Ilmu Komunikasi, FISIP, Universitas Bung Karno

Abstract: *Cyberwarfare has emerged as a national-security challenge alongside the expansion of digital infrastructure and networked communication. This conceptual study examines the meaning, actors, operational forms, vulnerabilities, and strategic responses associated with cyberwarfare in Indonesia. It uses a qualitative descriptive approach based on published national and international literature. Cyber threats can be conducted by state and non-state actors through hacking, sabotage, espionage, propaganda, attacks on information availability and integrity, malware, denial-of-service operations, and attacks on critical infrastructure. Indonesia's vulnerability is linked to its dependence on digital networks, uneven security governance, limited awareness, fragmented institutional responsibilities, technological dependence, and shortages of specialized personnel. The study proposes an integrated response involving legal certainty, coordinated governance under the National Cyber and Crypto Agency, qualified human resources, resilient infrastructure, standardized incident response, national and international cooperation, cyber diplomacy, and public digital-security awareness.*

Keywords: Cyberwarfare; Cybersecurity; National security; National Cyber and Crypto Agency; Cyber diplomacy

Abstrak: Perang siber berkembang menjadi tantangan keamanan nasional seiring meluasnya infrastruktur digital dan komunikasi berjaringan. Penelitian konseptual ini mengkaji makna, aktor, bentuk operasional, kerentanan, dan respons strategis terhadap perang siber di Indonesia. Penelitian menggunakan pendekatan deskriptif kualitatif berbasis literatur nasional dan internasional yang telah dipublikasikan. Ancaman siber dapat dilakukan aktor negara maupun nonnegara melalui peretasan, sabotase, spionase, propaganda, serangan terhadap ketersediaan dan integritas informasi, perangkat lunak berbahaya, denial-of-service, serta serangan terhadap infrastruktur kritis. Kerentanan Indonesia berkaitan dengan ketergantungan pada jaringan digital, tata kelola yang belum merata, rendahnya kesadaran, kewenangan kelembagaan yang terfragmentasi, ketergantungan teknologi, dan keterbatasan tenaga khusus. Penelitian menawarkan respons terpadu berupa kepastian hukum, koordinasi tata kelola di bawah Badan Siber dan Sandi Negara, penguatan SDM, infrastruktur tangguh, respons insiden yang baku, kerja sama nasional dan internasional, diplomasi siber, serta peningkatan kesadaran keamanan digital masyarakat.

Kata Kunci: Perang siber; Keamanan siber; Keamanan nasional; BSSN; Diplomasi siber

1. Pendahuluan

Era digital mengubah kehidupan sosial, ekonomi, pemerintahan, dan pertahanan melalui ketergantungan yang semakin besar pada teknologi informasi, komputer, dan jaringan internet. Perubahan tersebut meningkatkan efisiensi, tetapi sekaligus memperluas ruang serangan. Konflik tidak lagi terbatas pada wilayah fisik karena aktor dapat menyerang sistem informasi, komunikasi, layanan publik, dan infrastruktur strategis melalui ruang siber.

Perang siber telah menjadi isu keamanan internasional. Serangan terhadap Estonia pada 2007, konflik siber Korea Utara dan Korea Selatan, penggunaan Stuxnet, serta operasi spionase menunjukkan bahwa gangguan digital dapat berdampak pada lembaga pemerintah, sistem keuangan, media, dan fasilitas strategis (Badri, 2012; Soewardi, 2013). Sejumlah negara kemudian membangun komando, pusat operasi, dan unit khusus pertahanan siber.

Indonesia juga menghadapi serangan, penyusupan, dan ketegangan siber yang berkaitan dengan hubungan antarnegara maupun tindakan kelompok nonnegara. Ketergantungan pada layanan digital membuat keamanan siber tidak dapat dipisahkan dari keamanan nasional. Penelitian ini bertujuan menjelaskan karakter perang siber, memetakan kerentanan Indonesia, dan merumuskan respons yang dapat memperkuat ketahanan nasional.

2. Metode Penelitian

Penelitian menggunakan pendekatan deskriptif kualitatif dan bersifat konseptual. Objek kajian berupa tulisan yang telah diterbitkan dalam buku, jurnal, dan publikasi nasional maupun internasional mengenai perang siber, kejahatan siber, pertahanan siber, tata kelola, dan diplomasi siber. Literatur dibaca untuk mengelompokkan definisi, aktor, bentuk ancaman, sumber kerentanan, dan alternatif respons Indonesia.

Karena penelitian tidak menggunakan data insiden primer atau pengukuran kapasitas teknis, hasil tidak dimaksudkan sebagai audit operasional atas sistem keamanan tertentu. Angka pengguna internet, contoh serangan, dan kondisi kelembagaan diperlakukan sebagai konteks sebagaimana tersedia dalam sumber pada saat penelitian dilakukan.

3. Hasil dan Pembahasan

3.1. Makna dan Karakter Perang Siber

Perang siber berlangsung melalui ruang siber yang bersifat lintas batas, tidak terikat lokasi, dan dapat dijalankan pada berbagai waktu. Clarke dan Knake (2010) mendefinisikannya sebagai tindakan negara untuk menembus komputer atau jaringan negara lain dengan tujuan menimbulkan kerusakan atau gangguan. Dalam praktiknya, aktor nonnegara juga memiliki kemampuan melakukan operasi yang menghasilkan dampak strategis.

Tujuan serangan dapat berupa penguasaan, gangguan, penyesatan, pengaruh, penyanderaan, pencurian atau penghilangan informasi, pengalihan perhatian, penghentian komunikasi, dan penghancuran. Perang siber berbeda dari perang konvensional karena atribusi pelaku sulit dipastikan, biaya operasi relatif rendah, jangkauan serangan luas, dan sasaran dapat berupa sistem sipil maupun militer.

3.2. Aktor Perang Siber

Aktor perang siber dapat dikelompokkan menjadi aktor negara dan nonnegara. Aktor negara menggunakan kemampuan siber untuk kepentingan pertahanan, intelijen, diplomasi, atau tujuan geopolitik. Aktor nonnegara mencakup peretas individual, kelompok peretas, hacktivist, organisasi ekstremis, jaringan kejahatan terorganisasi, perusahaan, serta orang dalam yang memiliki akses terhadap sistem (Isnarti, 2016; Kallberg, 2016).

Kemampuan aktor bervariasi dari tingkat amatir hingga ahli keamanan informasi, spionase, forensik digital, analisis jaringan, dan operasi strategis. Karena alat serangan dapat digunakan lintas negara dan identitas pelaku dapat disamarkan, pembeda antara kejahatan siber, spionase, sabotase, dan perang siber sering bergantung pada tujuan, sasaran, skala dampak, serta hubungan pelaku dengan kepentingan negara.

3.3. Bentuk Ancaman Siber

Tabel 1: Bentuk Utama Ancaman Siber

Bentuk	Karakter Operasional
Peretasan dan cracking	Penerobosan sistem untuk mengakses, mencuri, mengubah, atau merusak data.
Sabotase	Gangguan atau penghancuran data, perangkat lunak, jaringan, komunikasi, dan infrastruktur.
Spionase	Pengumpulan informasi rahasia militer, politik, ekonomi, atau penelitian secara ilegal.
Propaganda	Pemanfaatan media digital untuk memengaruhi opini, persepsi, dan stabilitas sosial.
Cyber attack	Serangan terhadap kerahasiaan, integritas, atau ketersediaan informasi dan layanan.
Malware dan spyware	Program untuk menginfeksi, merekam aktivitas, memanipulasi, atau mengambil data.
Defacement dan DoS	Perusakan halaman web atau penghabisan sumber daya layanan agar tidak tersedia.
Infrastruktur kritis	Serangan pada listrik, transportasi, komunikasi, energi, dan layanan strategis.

Sumber: sintesis literatur dalam naskah sumber.

Ancaman terhadap perangkat keras dapat muncul melalui pemasangan komponen pengganggu atau manipulasi rantai pasok. Ancaman perangkat lunak menggunakan program untuk mencuri, merusak, atau memanipulasi informasi. Ancaman informasi bekerja melalui penyebaran atau pengubahan data untuk memengaruhi keputusan, opini publik, dan stabilitas sosial. Ketiganya dapat digunakan secara terpisah maupun dalam operasi hibrida (Othman, 2001; Rahmawati, 2017).

3.4. Kerentanan Indonesia

Kerentanan Indonesia meningkat karena layanan pemerintahan, ekonomi, komunikasi, energi, dan infrastruktur publik bergantung pada sistem informasi dan jaringan internet. Ardiyanti (2014) menempatkan tingginya penggunaan internet dan lemahnya manajemen keamanan sebagai faktor risiko. Ketergantungan teknologi dan terbatasnya penguasaan perangkat juga memengaruhi kemampuan membangun kemandirian pertahanan siber.

Faktor lain mencakup kesadaran keamanan yang belum merata, peralatan yang tidak selalu mengikuti perkembangan ancaman, ketidakhati-hatian terhadap perangkat lunak berbahaya, budaya kerja digital yang lemah, serta tata kelola kelembagaan yang sektoral. Chotimah (2019) menekankan pentingnya ketersediaan, integritas, dan kerahasiaan informasi sebagai dasar keamanan siber.

Kerawanan teknis dapat berkembang menjadi gangguan ekonomi, politik, sosial, dan pertahanan. Serangan terhadap listrik, telekomunikasi, transportasi, layanan keuangan, atau data pemerintahan dapat menimbulkan efek berantai. Propaganda dan manipulasi informasi juga dapat memperbesar ketidakpercayaan publik dan mengganggu stabilitas tanpa menggunakan kekuatan fisik.

3.5. Strategi Keamanan Siber Nasional

Tabel 2: Kerangka Respons Keamanan Siber Nasional

Dimensi	Prioritas
Hukum dan kebijakan	Memperjelas mandat, perlindungan infrastruktur kritis, kewenangan, dan respons insiden.
Tata kelola	Mengintegrasikan BSSN, TNI, Polri, kementerian, penyelenggara layanan, dan sektor strategis.
SDM	Membangun keahlian jaringan, perangkat lunak, forensik, intelijen, operasi, dan diplomasi siber.
Infrastruktur	Memperkuat pemantauan, pertahanan jaringan, pusat operasi, sistem informasi, dan fasilitas strategis.
Respons insiden	Menetapkan SOP, mekanisme tanggap, pertukaran informasi, latihan, dan pemulihan layanan.
Kerja sama	Mengembangkan kerja sama nasional, regional, bilateral, multilateral, dan jejaring tanggap insiden.
Kesadaran publik	Meningkatkan literasi keamanan, perlindungan data, disiplin penggunaan perangkat, dan pelaporan.

Sumber: sintesis rekomendasi dalam naskah sumber.

Kepastian hukum diperlukan untuk menetapkan mandat, kewenangan, mekanisme koordinasi, perlindungan infrastruktur kritis, dan tanggung jawab penanganan insiden. BSSN perlu menjadi simpul koordinasi yang menghubungkan kepolisian pada kejahatan siber, TNI pada pertahanan siber, Kementerian Luar Negeri pada diplomasi siber, Kementerian Komunikasi dan Informatika, serta lembaga lain yang mengelola layanan penting (Sa'diyah dan Vinata, 2016; Subagyo, 2015).

Penguatan SDM mencakup kemampuan perangkat lunak, jaringan, forensik digital, anti-peretasan, analisis informasi, telematika, operasi siber, serta manajemen insiden. Pembangunan kapasitas perlu berlangsung melalui pendidikan, pelatihan, latihan bersama, sertifikasi, penelitian, dan pengembangan karier. Kesiapan personel harus didukung infrastruktur pemantauan, perimeter defence, network monitoring, serta sistem pengelolaan informasi dan kejadian keamanan.

Kerja sama internasional dibutuhkan karena serangan dan infrastruktur digital bersifat lintas batas. Indonesia telah terlibat dalam forum regional dan global serta membangun kerja sama bilateral. Kerja sama perlu diarahkan pada pertukaran informasi, respons insiden, peningkatan kapasitas, pengembangan norma, dan diplomasi siber untuk melindungi kepentingan nasional sekaligus mengurangi risiko salah persepsi antarnegara.

3.6. Diplomasi dan Kesadaran Publik

Perang siber dapat berkembang ketika komunikasi internasional gagal dan hubungan antarnegara mengalami disharmoni. Diplomasi siber menjadi instrumen untuk membahas keamanan siber, kejahatan siber, confidence-building measures, kebebasan internet, dan tata kelola internet melalui jalur bilateral maupun multilateral. Diplomasi juga membantu membangun mekanisme tanggap insiden dan aturan perilaku yang dapat mengurangi eskalasi.

Pada tingkat masyarakat dan individu, keamanan nasional memerlukan kesadaran penggunaan perangkat, perlindungan identitas dan data, pembaruan sistem, kewaspadaan terhadap rekayasa sosial, serta pelaporan insiden. Kampanye dan pendidikan digital harus dipandang sebagai bagian dari pertahanan berlapis karena banyak serangan memanfaatkan kelemahan perilaku, bukan hanya kelemahan teknologi.

4. Kesimpulan

Perang siber merupakan ancaman terhadap keamanan, ketertiban, dan kedaulatan yang dapat dilakukan aktor negara maupun nonnegara melalui ruang siber. Bentuknya meliputi peretasan, sabotase, spionase, propaganda, serangan terhadap perangkat keras, perangkat lunak, informasi, layanan digital, dan infrastruktur kritis. Karakter lintas batas dan sulitnya atribusi membuat ancaman ini berbeda dari perang konvensional.

Indonesia menghadapi kerentanan akibat ketergantungan digital, penguasaan teknologi yang terbatas, kesadaran keamanan yang belum merata, tata kelola sektoral, dan kekurangan tenaga khusus. Respons nasional harus mengintegrasikan kepastian hukum, koordinasi kelembagaan, penguatan BSSN, SDM, infrastruktur, prosedur respons, perlindungan infrastruktur kritis, kerja sama internasional, diplomasi siber, dan pendidikan publik.

Penelitian berikutnya perlu menggunakan data insiden, pengukuran kematangan keamanan, analisis kapasitas lembaga, serta evaluasi efektivitas kerja sama agar rekomendasi konseptual dapat diuji terhadap kondisi operasional Indonesia.

Daftar Pustaka

Ardiyanti, Handrini. 2014. Cyber-Security dan Tantangan Pengembangannya di Indonesia. Politica, 5(1).

Badri, M. 2012. Perang Siber dalam Dinamika Komunikasi Internasional. Dalam Komunikasi Militer. Yogyakarta: Mata Padi Pressindo.

Chotimah, Hidayat Chusnul. 2019. Tata Kelola Keamanan Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara. Politica, 10(2).

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

Isnarti, Rika. 2016. A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War. Andalas Journal of International Studies, 5(2).

Kallberg, Jan. 2016. Strategic Cyber War Theory: A Foundation for Designing Decisive Strategic Cyber Operations. The Cyber Defense Review, 1(1).

Othman, Amarmuazam Usmani Bin. 2001. Analisis Penggunaan Media Siber terhadap Keamanan Nasional: Suatu Studi di Malaysia. Jurnal Prodi Strategi Pertahanan Darat, 3(3).

Rahmawati, Ineu. 2017. Analisis Manajemen Risiko Ancaman Kejahatan Siber dalam Peningkatan Cyber Defense. Jurnal Pertahanan dan Bela Negara, 7(2).

Sa'diyah, Nur Khalimatus dan Ria Tri Vinata. 2016. Rekonstruksi Pembentukan National Cyber Defence sebagai Upaya Mempertahankan Kedaulatan Negara. Perspektif, 21(3).

Subagyo, Agus. 2015. Sinergi dalam Menghadapi Ancaman Cyber Warfare. Jurnal Pertahanan, 5(1).

Soewardi, Bagus Artiadi. 2013. Perlunya Pembangunan Sistem Pertahanan Siber yang Tangguh bagi Indonesia. Media Informasi Ditjen Pothan Kemhan.

9 772615 074004 01