CYBER SECURITY DALAM STUDI KEAMANAN NASIONAL: POLITIK, HUKUM DAN STRATEGI

Oleh
Binsar Simorangkir[1], Tri Legionosuko[2], Surryanto Djoko Waluyo[3]
[1,2,3]Graduate School, Faculty of Defense Strategy, Indonesia Defense University
Jl. Sentul -Citeureup, Sentul, Kec. Citeureup, Bogor, Jawa Barat 16810, Indonesia
E-mail: [1*]Binsarau23@gmail.com, [2]Trilegionosuko@yahoo.co.id,
[3]Surryantodw_kemhan@yahoo.co.id

Abstrak

Tugas utama suatu negara adalah memastikan keamanan nasionalnya sendiri. Ketika suatu negara dapat memastikan kelangsungan hidupnya sendiri dan mata pencaharian warganya, negara itu dianggap kuat. Namun, dunia berubah dengan cepat, dan penemuan serta teknologi baru menghadirkan peluang dan risiko bagi keamanan nasional. Artikel ini berusaha menunjukkan bagaimana studi keamanan nasional telah berkembang dalam hal politik, legislasi, dan taktik. Dalam posting ini, metodologi analisis konten akan diterapkan. Dapat disimpulkan dari lebih dari 20 studi yang dikutip di sini bahwa revolusi industri terbaru, yang dikenal sebagai industri 4.0, memiliki dampak signifikan terhadap perubahan lingkungan strategis. Dengan demikian, ini menciptakan kesulitan baru seperti serangan dunia maya. Peneliti sampai pada kesimpulan bahwa bahaya ini mungkin memiliki implikasi strategis bagi suatu negara. Bahaya ini kemudian berpusat pada bahaya politik terhadap keamanan kolektif, bahaya hukum yang membutuhkan legislasi dunia maya, dan bahaya strategis yang membutuhkan keamanan dunia maya.

Kata Kunci: Keamanan Siber, Keamanan Nasional, Strategi, Politik, Hukum

PENDAHULUAN

Dengan sejumlah kemajuan yang membuat pemenuhan kebutuhan manusia menjadi lebih sederhana dan menyenangkan, teknologi digital era industri 4.0 telah merevolusi cara hidup. Digitalisasi informasi memudahkan untuk membangun jaringan yang membentuk suatu sistem. Untuk keperluan pengumpulan data, analisis data, evaluasi pengembangan usaha, dan peningkatan kinerja, produk mereka sendiri dimasukkan ke dalam satu jaringan terpadu. Untuk menganalisis bagaimana Industri 4.0 akan memengaruhi bisnis, kita harus menggunakan rantai nilai yang sangat membantu [1]. Sayangnya, kemajuan teknologi ini tidak hanya menciptakan kemungkinan dan kemudahan baru tetapi juga bahaya baru. Risiko potensial dan masalah keamanan tidak diberi bobot yang sama dengan produktivitas dan kualitas produksi.

Setiap negara memiliki seperangkat kebijakan unik yang telah dikembangkan untuk mengamankannya, menurut penelitian keamanan nasional. Peraturan ini mencakup berbagai bidang, termasuk politik, ekonomi, sosial, dan budaya. Peraturan-peraturan ini harus diperbarui dan dimodifikasi dengan mempertimbangkan kemajuan teknologi yang dibawa oleh revolusi industri untuk mengatasi masalah keamanan saat ini. Pertumbuhan bidang kehidupan yang terkena dampak revolusi industri membutuhkan ide dan pendekatan baru untuk mengatasi ancaman yang sudah ada. Pergeseran inilah yang mengubah tujuan dari studi keamanan nasional itu sendiri.

Dari perspektif suatu negara, perubahan global menyebabkan lingkungan strategis berubah dengan cepat. Untuk dapat mengatasi perubahan lingkungan strategis ini, setiap negara harus mengambil inisiatif. Digitalisasi sistem adalah perkembangan utama yang dihasilkan dari revolusi industri keempat. Dengan kemudahan teknologi informasi modern, negara-negara memiliki kecenderungan untuk bekerja sama secara regional untuk mengatasi masalah antar negara, seperti keamanan dan ekonomi. Prioritas geopolitik dalam perilaku negara memicu perdebatan baru tentang tatanan dunia.

Gagasan baru dalam keamanan nasional diperkenalkan oleh transformasi dalam lingkungan strategis ini. Hari-hari ini, ide-ide yang muncul seperti keamanan dunia maya, keamanan kolektif, dan hukum dunia maya sering menjadi berita. Kemampuan suatu negara untuk melindungi keamanannya kini menghadapi tantangan baru dari sektor teknologi dan dunia online. Ketiga konsep baru ini perlu dibenahi karena dikonseptualisasikan sesuai dengan sektornya masing-masing: keamanan kolektif sebagai ancaman di bidang politik, keamanan siber sebagai ancaman di bidang strategi, dan hukum siber sebagai ancaman. Ketiga konsep baru ini sesuai dengan pandangan neorealis, yaitu konseptualisasi target teoritis yaitu keamanan dan ancaman negara, dan asumsi anarkis (*security dilemma*) [2].

LANDASAN TEORI

Keamanan Nasional

Keamanan nasional merupakan kebutuhan mendasar untuk mempertahankan dan mempertahankan kepentingan negara atau negara dengan memanfaatkan kekuatan politik, ekonomi, dan militer untuk menangkal ancaman baik di dalam maupun di luar negeri. Kebutuhan untuk menjaga dan menegakkan eksistensi Negara melalui kekuatan ekonomi, militer, dan politik, serta pertumbuhan diplomasi, adalah cara lain untuk mendefinisikan keamanan nasional. Kemampuan pemerintah untuk mempertahankan keutuhan wilayah negara terhadap ancaman eksternal dan internal ditekankan dalam gagasan ini.

Arnold Wolfers menyatakan bahwa keamanan berarti mengukur tidak adanya ancaman terhadap nilai-nilai yang dicapai, dalam pengertian subjektif [3]. Tidak ada kekhawatiran bahwa prinsip-prinsip ini akan ditentang. Keamanan didefinisikan sebagai tidak adanya bahaya terhadap cita-cita yang dibutuhkan orang untuk menjalankan kehidupannya. kemampuan suatu negara untuk melindungi diri dari segala ancaman guna menjaga keamanan nasional.

Barry Buzan menegaskan bahwa ada tiga tingkat keamanan dalam kaitannya dengan isu-isu yang berkaitan dengan kehidupan manusia: keamanan pribadi (juga dikenal sebagai keamanan manusia), keamanan pemerintah, dan keamanan internasional. Melindungi keamanan rakyat akan segera menghasilkan keamanan nasional karena keamanan nasional dan kesejahteraan manusia saling terkait erat. Perlindungan warganya adalah kewajiban negara.

Fokus keamanan nasional adalah pada kebijakan pemerintah yang menggunakan kekuatan ekonomi, kekuatan militer, dan diplomasi baik dalam perdamaian maupun konflik untuk menjamin keselamatan dan keamanan negara. Untuk mencapai keamanan nasional suatu negara, teknik yang digunakan untuk menjaga keamanan termasuk menggunakan diplomasi untuk mengidentifikasi sekutu dan mengisolasi bahaya serta menggunakan kekuatan ekonomi untuk bekerja dengan negara lain. Untuk mempertahankan kekuatan militer yang efisien, beberapa negara penting saat ini bekerja sama baik secara langsung maupun tidak langsung [4]. Penggunaan dan pemanfaatan kekuatan militer merupakan salah

satu cara untuk menjamin keamanan suatu negara.

Keberlangsungan Negara dan mempertahankan Negara dan Bangsa dari bahaya merupakan komponen penting dari Kepentingan Nasional. Kepentingan nasional dapat dibingkai sebagai tujuan yang ingin dicapai sehubungan dengan keutuhan bangsa/negara [5].

Konsep Siber dalam Keamanan Nasional

Istilah "keamanan siber" atau "*cyber security*" merupakan istilah yang memiliki beberapa definisi dan penerapan yang berbeda. Karena dunia maya, lingkungan virtual yang tercipta dari perpaduan manusia dan teknologi, adalah tempat yang nyata. Teknologi informasi dan komunikasi adalah yang dimaksud [6]. Oleh karena itu, gagasan keamanan dunia maya kini memengaruhi lebih dari sekadar teknologi dan menimbulkan risiko bagi keamanan nasional.

Konsep keamanan telah berubah secara signifikan akibat perkembangan teknologi informasi; ruang interaksi kini tidak hanya terbatas pada dunia fisik tetapi juga mencakup dunia maya (*cyber*). Oleh karena itu, negara harus menyesuaikan diri dengan pertumbuhan ini. Sudah saatnya gagasan keamanan siber diakui sebagai salah satu “wilayah” negara, dengan kewajiban negara untuk melindungi wilayahnya tetap berlaku. Tujuan keamanan siber adalah untuk mengatasi masalah keamanan informasi untuk kegiatan pemerintah, nirlaba, dan pribadi yang melibatkan teknologi TIK, khususnya teknologi internet [7].

Cybersecurity dan "keamanan informasi" adalah dua ide yang berbeda. Dalam hal perlindungan aset, menggagalkan spionase bisnis dan industri, memerangi terorisme dan bentuk kejahatan ekonomi lainnya, serta mencegah akses ke materi yang tidak dapat diterima, ada konsensus umum di beberapa tempat [7]. Keduanya merupakan dua konsep yang berbeda dalam pengaturan yang berbeda. *Cybersecurity* mencakup semua aspek pemantauan komputer, pengawasan, pembatasan yang sangat ketat, dan pembelaan hak asasi manusia. Sedangkan keamanan informasi terkait dengan isu-isu yang lebih umum seperti kedaulatan negara, keamanan nasional, pengamanan infrastruktur vital, pengamanan aset baik kasat mata maupun kasat mata, pengamanan data pribadi, dan lain-lain [7].

METODE PENELITIAN

Dalam penelitian ini, digunakan analisis isi sebagai metodologi penelitian yang. Ketika peneliti meneliti komunikasi dari manusia, seperti buku, teks, esai, surat kabar, jurnal, artikel, musik, majalah, jurnal, atau komunikasi lain yang mungkin diteliti, mereka secara tidak langsung mempelajari perilaku manusia. Analisis adalah metode kajian yang berkonsentrasi pada struktur internal dan konteks eksternal media. Ini akan digunakan nanti untuk memastikan apakah kata, konsep, tema, frasa, karakter, atau kalimat tertentu ada dalam teks. Teks dapat dibaca sebagai berita, jurnal, dialog, obrolan, dokumen sejarah, iklan, dan jenis publikasi lainnya.

Analisis konten biasanya digunakan untuk menganalisis data kualitatif dan kredibel yang sering disajikan menggunakan istilah seperti kredibilitas, ketergantungan, kesesuaian, transferabilitas, dan keaslian. Artikel ini berfokus pada keyakinan yang memperluas studi keamanan dengan memasukkan perkembangan politik, hukum, dan strategis. Informasi tersedia untuk pemerintah dan masyarakat umum, memungkinkan mereka untuk mempengaruhi masyarakat dan negara. Berdasarkan review dari studi sebelumnya dan buku teks metodologis yang dapat diandalkan untuk tahap analisis konten, dari pengumpulan data hingga hasil pelaporan. Dapat disimpulkan bahwa harus diuji keterandalan setiap tahap proses analitis, termasuk persiapan, pengorganisasian, dan pelaporan hasil [8].

HASIL DAN PEMBAHASAN

Dengan munculnya teknologi informasi, yang dibawa oleh revolusi industri terbaru, keamanan nasional kini telah menyebar dan meluas. Karena teknologi informasi sudah begitu lekat dengan kehidupan manusia, maka tidak hanya masalah keamanan informasi yang menghadapi tantangan baru akibat keberadaannya, tetapi ancaman baru perang asimetris yang dipicu oleh penyebaran terorisme juga memprihatinkan [9]. Strategi pertahanan tradisional tidak mampu mengantisipasi pergeseran ini. Pertumbuhan ini terlihat pada sektor-sektor utama, yaitu politik, hukum, dan strategi.

Gerakan politik global mulai bergeser ke arah regionalisme. Hal ini karena aspek politik, khususnya kecenderungan negara membentuk organisasi regional yang fokus pada satu atau beberapa isu. Hal ini dibuktikan dengan terbentuknya organisasi seperti *Association of Southeast Asian Nations, North America Treaty Organization, Shanghai Cooperation Organization*, dan masih banyak lagi. Formasi organisasi daerah ini dibatasi oleh keamanan kolektif.

Pakar hubungan internasional menyebut negara-negara yang bekerja sama untuk menjaga kepentingan masing-masing negara sebagai berpartisipasi dalam "keamanan kolektif". Perserikatan Bangsa-Bangsa, terkadang dikenal sebagai Perserikatan Bangsa-Bangsa, adalah salah satu lembaga paling terkenal di masyarakat dalam skala global. Negara-negara yang menandatanganinya bekerja sama untuk memajukan kepentingan nasional masing-masing, termasuk melindungi keamanan nasional. Ini bukan hal baru, tetapi kecenderungan kerjasama regional antar negara adalah yang menjadi perhatian geopolitik.

Hukum siber diperlukan di bidang hukum bagi negara untuk menerapkan aturan dalam rangka menjaga keamanan nasional. Dasar hukum bagi negara untuk menindak pelanggaran adalah *cyber law*. Hal ini diperlukan sebagai bentuk upaya negara untuk menjaga keamanan nasional.

Selain hukum siber, prospek pertumbuhan teknologi informasi juga terancam. Pemerintah di seluruh dunia mulai menggunakan informasi yang baru ditemukan ini untuk menciptakan prosedur pemerintahan yang lebih akuntabel, transparan, dan berpusat pada warga negara. Upaya e-government yang sukses secara global dimungkinkan oleh infrastruktur teknologi informasi dan komunikasi yang saat ini ada dan persetujuan pemerintah untuk melaksanakan e-governance. Bahkan jika beberapa negara berkembang telah membuat kemajuan ke arah ini, mereka seringkali gagal dalam hal meningkatkan kerangka tata kelola dan hasil yang berkelanjutan. Agar negara-negara miskin dapat mencapai tujuan *e-government* mereka, berbagai hambatan harus dikenali dan dihilangkan [10]. Oleh karena itu, bahaya ini memengaruhi semua organisasi, baik itu organisasi ekonomi, sosial, atau kemanusiaan dan tidak hanya organisasi di sektor keamanan. Hal ini disebabkan pola keakraban yang dikembangkan melalui kerjasama organisasi, yang menjadi ancaman bagi negara-negara di luar kawasan.

Di bidang strategi, merebaknya dunia siber sebagai akibat dari kemajuan teknologi informasi. Ini menciptakan dilema baru bagi pemerintah, yaitu keamanan siber. Digitalisasi telah menjadi ranah baru bagi negara-negara untuk menjaga keamanan nasionalnya karena teknologi informasi telah mengintegrasikan seluruh aspek kehidupan. Saat ini, strategi kedaulatan dan otonomi dianggap berada di bawah ancaman dari meningkatnya ketegangan internasional, transformasi digital yang mengganggu, dan peningkatan insiden keamanan siber. Persimpangan AI dan keamanan siber berada di garis depan perkembangan ini, menimbulkan banyak pertanyaan dan dilema etis. Masalahnya adalah

bagaimana memahami etika AI dan cybersecurity dalam kaitannya dengan strategi kedaulatan dan otonomi [11].

Keamanan siber suatu negara menunjukkan kesiapannya menghadapi era ini. Digitalisasi berbagai aspek kehidupan tidak luput dari perhatian aparat keamanan suatu negara. Salah satu contohnya adalah kasus penyadapan telepon Australia terhadap salah satu presiden Indonesia. Penyadapan dilakukan dengan menggunakan telepon genggam Presiden Indonesia saat itu, Susilo Bambang Yudhoyono. Kasus ini bahkan diliput oleh media internasional, yang sayangnya menunjukkan kelemahan pertahanan siber Indonesia.

Penyadapan hanyalah salah satu jenis ancaman dunia maya. Spionase, pencurian informasi, dan bahkan kejahatan transnasional kini dapat dilakukan kapan saja dan dari lokasi mana saja. Siapa pun dapat melancarkan serangan, mencuri informasi, dan bahkan terlibat dalam kejahatan transnasional seperti perdagangan gelap. Banyak negara berkembang tidak memiliki pertahanan dunia maya yang memadai dari sudut pandang keamanan nasional. Selain kasus di Indonesia, masih banyak serangan siber terhadap negara yang merugikan negara dan menjadi ancaman nyata bagi negara.

Namun, penggunaan teknologi untuk pertahanan bukanlah konsep baru. Banyak pemerintah di seluruh dunia sudah menggunakan teknologi untuk meningkatkan keamanan negara mereka. Berikut adalah beberapa cara berbagai negara menggunakan teknologi untuk melindungi keamanan nasional mereka.

Amerika Serikat menggunakan teknologi dalam berbagai cara untuk melindungi diri dan kepentingannya, termasuk memantau lalu lintas Internet dan komunikasi online. Pemerintah juga melacak panggilan telepon untuk memantau potensi ancaman keamanan.

Rusia juga menggunakan berbagai teknologi untuk memantau komunikasi dan memerangi terorisme. Ini menggunakan sistem yang dikenal sebagai *System for Operative Investigative Activities* (SORM; Russian: *Система оперативно-разыскных мероприятий*) untuk melacak panggilan telepon dan memantau aktivitas di Internet. Demikian pula, China memiliki sistem serupa untuk menjaga warganya di bawah pengawasan ketat dan mencegah serangan teroris. Itu juga menggunakan perangkat lunak pengenal wajah untuk mengidentifikasi orang-orang di area publik dan memantau perilaku mereka. Selain itu, ia memelihara jaringan besar kamera CCTV yang memantau jutaan orang setiap hari.

Iran juga menggunakan berbagai cara untuk memantau aktivitas warganya. Ini memiliki jaringan kamera CCTV di kota-kota besar untuk mengawasi warganya. Ini juga memiliki sistem teleskrin nasional untuk memantau panggilan telepon dan aktivitas lain yang dilakukan oleh warga.

Inggris memiliki berbagai tindakan untuk mencegah serangan teror dan melindungi diri dari ancaman pelanggaran keamanan dunia maya. Ini memiliki undang-undang ketat yang berkaitan dengan privasi data dan keamanan digital dan memantau aktivitas warganya secara teratur. Misalnya, di bawah Undang-Undang Terorisme tahun 2000, individu yang bepergian ke luar negeri untuk melakukan tindakan terorisme atau mendapatkan pelatihan teroris adalah ilegal. Itu juga memelihara basis data DNA nasional yang digunakan untuk membandingkan badan tak dikenal dengan yang ada dalam register untuk mengidentifikasi kemungkinan kecocokan. Ia juga memiliki jaringan kamera CCTV di seluruh kota besar untuk memantau aktivitas dan pergerakan warganya. Ini juga memiliki beberapa program untuk melatih analis dunia maya baru dan mendukung personel yang ada dalam perjuangan mereka melawan serangan dunia maya.

PENUTUP

Kesimpulan

Efek pertumbuhan industri di era 4.0 melampaui bidang bisnis dan industri hingga masalah keamanan. Oleh karena itu, negara dituntut untuk mengubah tantangan keamanan dari masalah yang hanya berdampak pada dirinya menjadi masalah global. Akibatnya, negara beradaptasi dengan mengubah kerangka hukum, politik, dan strategis untuk mengatasi bahaya yang tidak terduga dan tidak pernah terdengar. Kesenjangan masalah keamanan nasional disebabkan oleh ketidakmampuan negara-negara berkembang untuk menangani masalah baru di era industri 4.0. Pengenalan gagasan-gagasan baru seperti keamanan siber dan hukum siber, serta pola interaksi global yang telah bergeser ke arah regionalisme dan keamanan kolektif, telah membuka berbagai potensi risiko di tingkat nasional suatu negara.

Jika masalah ini tidak segera diselesaikan, dapat menyebabkan eksploitasi dan isolasi suatu bangsa, baik di tingkat hubungan internasional maupun di tingkat individu dalam masyarakat yang terpapar bahaya dunia maya. Untuk mengatasi agenda keamanan nasional yang berkembang ini, diperlukan penilaian strategi yang menyeluruh. Rahasia sukses di masa depan adalah menguasai bidang teknologi informasi yang terus berkembang.

DAFTAR PUSTAKA

[1] Nagy, J., Oláh, J., Erdei, E., Máté, D., & Popp, J. (2018). The role and impact of industry 4.0 and the internet of things on the business strategy of the value chain-the case of Hungary. *Sustainability (Switzerland)*, *10*. https://doi.org/10.3390/su10103491

[2] Mearsheimer, J. J. (1995). A realist reply. *International security*, *20*(1), 82-93.

[3] Wolfers, A. (1962). *Discord and collaboration: essays on international politics*. Baltimore: Johns Hopkins Press.

[4] Pinto. 2007. Keamanan nasional-Antara Ancaman Internal dan eksternal TIMOR LESTE. Penerbit : ETTIS.

[5] Rudi, T.May. 2002. *Studi STRATEGIS: Dalam transformasi Sistem Internasional Pasca Perang dingin*

[6] Sitompul, Josua. 2012. *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*. Jakarta: PT. Tatanusa.

[7] Ghernaouti, Solange. 2013. *Cyber Power: Crime, Conflict and Security in Cyberspace*. Lausanne: EPFL Press.

[8] Elo, Satu, et al. "Qualitative content analysis: A focus on trustworthiness." *SAGE open* 4.1 (2014): 2158244014522633.

[9] Mallik, Amitav. (2004). *Technology and 21st Century a Demand-Side Perspective* (Issue 20).

[10] As-Saber, S. N., Srivastava, A., & Hossain, K. (2006). *Information Technology Law and E-government: 1*(1).

[11] Timmers, P. (2019). Ethics of AI and Cybersecurity When Sovereignty is at Stake. *Minds and Machines*, *29*(4). https://doi.org/10.1007/s11023-019-09508-4