Jurnal Diplomasi Pertahanan,
Volume 6, Nomor 3, 2020 E-ISSN 2746-8496

Memperluas Agenda Studi Keamanan Nasional: Politik, Hukum dan Strategi

Expanding the Agenda for National Security Studies: Politics, Law and Strategy

Binsar Simorangkir

Perwira Polisi Militer (POM) TNI AU

Binsar@idu.ac.id

Abstract

National security is the first and foremost responsibility of a nation. A nation is considered a strong nation once it is able to secure the livelihood of the people and the wellbeing of the nation itself. Yet the world is evolving quickly and new technologies and innovations bring about new threats and opportunities towards national security. This article aims to describe the expansion of politics, laws, and strategies within the study of national security. Content analysis method will be used in this article. From more than 20 articles referenced here, it can be summarized that changes in strategic environment is heavily affected by the latest industrial revolution, the industry 4.0. Thus, this brings about new challenges such as cyber threats. The researcher then concluded that these threats could affect a nation strategically. These threats then focused on political threats of collective security, current law threats which requires cyber law, and strategic threats which is cyber security.

Keywords*: National Security, Strategy, Politic, Law*

1. Pendahuluan

Teknologi informasi era industri 4.0 dewasa ini telah merubah cara hidiup lebih mudah dengan beragam inovasi untuk memenuhi kebutuhan umat manusia semakin lebih mudah dan menyenangkan. Digitalisasi informasi memudahkan terciptanya sebuah jaringan yang membentuk sistem. Produk mereka sendiri diintegrasikan ke dalam satu jaringan terintegrasi untuk pengumpulan data, analisis data, evaluasi pengembangan perusahaan, dan peningkatan kinerja. Untuk mempelajari dampak Industri 4.0 pada perusahaan tempat kami menggunakan rantai nilai yang sangat berguna (Nagy et al., 2018). Sayangnya, kemajuan teknologi ini tidak hanya membawa kesempatan dan kemudahan yang baru, melainkan juga membawa ancaman-ancaman baru. Kemungkinan bahaya dan ancaman keamanan tidak dilihat dalam ukuran yang sama bersama dengan efisiensi produksi dan produktivitas. Pengembangan industri manufaktur inovatif dan generasi peralatan dan teknologi berikutnya yang tidak memiliki ukuran keamanan yang tepat sebagai bagian integral dari desain bahaya yang terus meningkat bagi industri yang ingin mengadopsi teknologi tersebut. Akibatnya, evolusi spektrum luas dari serangan fisik cyber unik yang bertujuan mengganggu dan mungkin mungkin menyabotase entitas industri manufaktur menjadi minat dan prioritas utama penyerang fisik cyber (Prinsloo et al., 2019).

Dalam konteks studi keamanan nasional, setiap negara memiliki agenda kebijakan masing-masing untuk mengamankan negaranya. Kebijakan-kebijakan ini meliputi berbagai sektor, seperti politik, ekonomi, sosial, dan budaya. Dengan berkembangnya teknologi yang dibawa dengan revolusi industri, kebijakan-kebijakan ini perlu dirubah dan disesuaikan untuk menjawab tantangan keamanan di masa kini. Perubahan inilah yang mengubah agenda dari studi keamanan nasional sendiri, ekspansi dari sektor-sektor kehidupan yang terpengaruhi dalam revolusi industri menuntut pemikiran dan pola baru untuk menghadapi ancaman yang ada.

Dari sudut pandang negara, perubahan-perubahan di dunia membuat lingkungan strategis disekitarnya bertransformasi dengan cepat. Hal ini menuntut sebuah inisiatif dari setiap negara untuk mampu mengatasi perubahan lingkungan strategis ini. Perubahan paling besar yang dibawa oleh revolusi industri 4.0 ini adalah digitalisasi sistem. Dengan dengan kemudahan sistem informasi sekarang, terdapat kecenderungan negara-negara untuk bergabung secara regional untuk menghadapi isu antar negara, seperti keamanan dan ekonomi. Perilaku negara yang cenderung mengutamakan geopolitik, membuat sebuah polemik baru dalam tatanan global.

Perubahan lingkungan strategis ini membawa konsep baru bagi keamanan nasional. Konsep-konsep baru seperti *cyber security*, *collective security*, dan *cyber law* seringkali menjadi sorotan di masa kini. Sektor teknologi dan sebuah dunia siber menjadi tantangan baru bagi sebuah negara dalam mempertahankan keamanannya. Ketiga konsep baru ini sesuai dengan pandangan neorealis, yaitu konseptualisasi target-target teoritis yaitu keamanan (*state security*) dan ancaman (*threat*) dan asumsi anarkis (*the security dilemma*)(Walt 1991:212; Posen 1993a:82; Schultz, Godson, dan Greenwood 1993:2; Mearsheimer 1995). konsep-konsep baru ini membutuhkan jawaban, karena konseptualisasi ketiganya tertuang sesuai dengan sektor masing-masing, yaitu *collective security* sebagai ancaman di bidang politik, *cyber security* sebagai ancaman di bidang strategi, dan *cyber law* sebagai ancaman di bidang hukum.

2. Tinjauan Pustaka

2.1 Keamanan Nasional

Keamanan nasional diartikan sebagai kebutuhan dasar untuk melindungi dan menjaga kepentingan nasional suatu bangsa yang bernegara dengan menggunakan kekuatan politik, ekonomi, dan militer untuk menghadapi berbagai ancaman, baik yang datang dari dalam maupun dari luar negeri. (Praditya 2016) Keamanan nasional juga dapat diartikan kebutuhan untuk memelihara dan mempertahankan eksistensi Negara melalui kekuatan ekonomi, militer, dan politik, serta pengembangan diplomasi. Dalam konsep ini yang ditekankan adalah kemampuan pemerintah dalam melindungi integritas teritorial negara dari ancaman yang datang dari luar dan dari dalam negara.

Definisi Keamanan yang lebih komprehensif oleh Arnold Wolfers (1962) bahwa *Security, in any objectives sense, measures the absence of threat to acquired values, in a subjectives sense. The absence of fear that such values will be attacked.* Dijelaskan bahwa keamanan merupakan ketiadaan ancaman nilai-nilai yang dibutuhkan manusia dalam menjalani kehidupannya. Kemampuan suatu Negara untuk membebaskan bangsanya dari segala bentuk ancaman untuk mempertahankan Keamanan nasional.

Menurut Barry Buzan, ada tiga tingkatan keamanan dalam problem kehidupan manusia, yaitu keamanan Individu (*Human Security*), Keamanan Nasional dan Keamanan Internasional. Keamanan Nasional erat kaitannya dengan kesejahteraan masyarakat, maka dengan melindungi keamanan masyarakat dengan sendirinya akan tercapai keamanan nasional. Tugas negara untuk melakukan perlindungan terhadap rakyatnya.

Keamanan Nasional menitik beratkan pada kebijakan publik untuk memastikan keselamatan dan keamanan negara melalui penggunaan kekuatan ekonomi, militer, perjalanan diplomasi, baik dalam keadaan damai maupun perang. Cara yang digunakan untuk melindungi keamanan suatu negara antara dengan cara menggunakan diplomasi untuk mencari sekutu dan mengisolasi ancaman, menggunakan kekutan ekonomi untuk melakukan kerja sama dengan negara lain guna tercapainya keamanan nasional suatu

Negara. Saat ini banyak Negara-negara besar melakukan kerja sama dengan negara lain baik secara langsung maupun tidak langsung untuk melakukan kerja sama, dan menjaga angkatan bersenjata yang efektif (Pinto, 2007). Untuk menjamin keamanan suatu Negara dapat dilakukan melalui penggunaan dan pemanfaatan kekuatan angkatan bersenjata.

Kepentingan Nasional erat kaitannya dengan kelanjutan Negara dan melindungi Negara dan Bangsa dari ancaman. Menurut T. May Rudi (2001:16) bahwa kepentingan nasional dapat dirumuskan sebagai tujuan-tujuan yang ingin dicapai sehubungan dengan keutuhan bangsa/negara atau yang dicita-citakan.

2.2 Memahami Konsep *Cyber* dalam konteks Keamanan Nasional

Ada banyak terminologi dan interpretasi yang dihubungkan dengan konsep "cyber security" atau "keamanan cyber". Karena cyberspace merupakan ruang virtual yang terbentuk dari hasil penyatuan antara manusia dan teknologi. Teknologi yang dimaksud ialah teknologi informasi dan komunikasi (Sitompul, 2012: 15). Maka konsep keamanan cyber tidak lagi hanya menyentuh wilayah teknologi tapi telah menjadi ancaman terhadap keamanan nasional.

Perkembangan teknologi informasi juga telah memberikan perubahan signifikan mengenai konsep keamanan, kini ruang interaksi tidak bisa hanya dibatasi seara fisik (physic) tapi juga meluas ke dunia maya (cyber). Konsekuensinya, negara harus beradaptasi dengan perkembangan ini konsep keamanan dunia maya (cyber security) sudah saatnya ditetapkan sebagai salah satu "wilayah" negara yang jaga keamanannya sebagaimana kewajiban negara mengamankan teritorialnya. Keamanan cyber ditujukan pada isu keamanan informasi bagi pemerintahan, organisasi dan urusan individual yang dihubungkan dengan teknologi ICT, dan secara khusus dengan teknologi internet (Ghernaouti, 2013:329).

Terminologi "keamanan informasi (information security)" dan keamanan cyber adalah dua konsep berbeda. Dalam konteks tertentu ada kesamaan pemahaman jika dikaitkan dengan proteksi aset atau perlawanan terhadap spionase industri dan ekonomi, perlawanan terhadap terorisme atau kejahatan ekonomi, perlawanan tehadap konten-konten terlarang (Ghernaouti, 2013: 330).

Dalam konteks lain, dua konsep tadi memiliki perbedaan. Keamanan cyber mencakup segala sesuatu berhubungan dengan pengawasan komputer, monitoring sampai kontrol yang sangat ketat atau perjuangan untuk hak asasi fundamental.

Sedangkan keamanan informasi berhubungan dengan isu-isu yang lebih luas, seperti kedaulatan negara, keamanan nasional, proteksi atas infrastruktur penting, keamanan aset-aset yang terlihat maupun yang tidak terlihat, dan proteksi data personal dan sebagainya (Ghernaouti, 2013: 330)

3. Metode Penelitian

Metode penelitian yang digunakan dalam artkikel ini adalah content analysis. Dimana peneliti dalam mengkaji perilaku manusia secara tidak langsung melalui analisis terhadap komunikasi mereka seperti buku, teks, essay, koran, novel, artikel, lagu, majalah, jurnal, ataupun komunikasi lain yang dapat dianalisis. Analisis merupakan sebuah alat penelitian yang difokuskan pada kontek aktual dan fitur internal media. Nantinya akan digunakan untuk menentukan keberadaan kata-kata tertentu, konsep, tema, frase, karakter, atau kalimat dalam teks. Teks dapat diartikan sebagai, berita, buku, jurnal, wawancara, diskusi, dokumen sejarah, percakapan, iklan, dokumen lain.

Analisis Konten biasanya digunakan untuk menganalisis data kualitatif, dapat dipercaya sering kali disajikan oleh menggunakan istilah-istilah seperti kredibilitas, ketergantungan, kesesuaian, pengalihan, dan keaslian. Artikel ini berfokus pada kepercayaan bahwa perluasan studi keamanan dengan dengan perkembangan politik,

hukum dan strategi. Pemerintah maupun masyarakat luas memiliki akses terhadap informasi, memepengaruhi masyarakat dan negara. Berdasarkan tinjauan studi sebelumnya, pengalaman kami sendiri, dan buku teks metodologis dapat dipercaya untuk tahap analisis isi dari pengumpulan data hingga pelaporan hasil. Kami menyimpulkan untuk meneliti keterpercayaan setiap fase proses analisis, termasuk persiapan, organisasi, dan pelaporan hasil. Bersama-sama, fase-fase ini harus memberi pembaca indikasi yang jelas tentang keseluruhan kepercayaan pembelajaran. Berdasarkan temuan dari data kemi mencoba memahami bahwa perluasan studi keamanan nasional sangat penting.(Elo et al., 2014)

4. Hasil dan Diskusi

Keamanan nasional kini telah merebak dan meluas dengan adanya teknologi informasi yang dibawa oleh revolusi industri terkini. Teknologi informasi telah menjadi begitu intrinsik bagi kehidupan manusia sehingga bukan hanya masalah keamanan informasi menghadapi tantangan baru dari keberadaan teknologi, namun ancaman baru perang asimetris yang dipicu oleh penyebaran terorisme yang mengkhawatirkan. (Amitav Mallik, 2004) Strategi pertahanan konvensional tidak mampu mengantisipasi perubahan ini. Adapun perluasan ini bisa terlihat dari sektor-sektor besar yaitu politik, hukum dan strategi.

Pada sektor politik, terlihat pergerakan dunia yang mulai mengarah kearah regionalisme. Hal ini disebabkan dari aspek politis yaitu adanya kecenderungan bagi negara-negara untuk membentuk suatu organisasi regional yang berfokus pada satu isu atau lebih. Hal ini tampak dari pembentukan A*ssociation of Southeast Asean Nation* (ASEAN), *Shanghai Cooperation Organization*, dan banyak lagi. Pembentukan-pembentukan organisasi regional ini memiliki warna yang sama, yaitu didasari oleh keamanan kolektif atau *collective security.*

Collective security merupakan terminologi yang digunakan oleh penstudi HI untuk menyebutkan negara-negara yang bersatu untuk mengamankan kepentingan setiap negaranya. Secara global, salah satu organisasi yang sudah awam di masyarakat adalah PBB atau perserikatan bangsa-bangsa. Negara-negara yang bergabung di dalamnya, bersama-sama berupaya untuk mengejar kepentingan nasional, yaitu menjaga keamanan nasional masing-masing. Hal ini bukanlah hal yang baru, tetapi, dengan adanya tren yang cenderung membuat negara-negara berkumpul secara regional inilah yang membuat ancaman geopolitik terjadi.

Pada sektor hukum, diperlukan adanya *cyber law* bagi negara untuk melaksanakan aturan-aturan demi menjaga keamanan nasional. *Cyber law* atau hukum siber ini menjadi dasar hukum bagi negara untuk melakukan tindakan-tindakan atas pelanggaran-pelanggaran yang terjadi. Hal ini diperlukan sebagai bentuk upaya negara untuk menjaga keamanan nasionalnya.

Selain *cyber law*, peluang pengembangan melalui teknologi informasi juga terancam. Pemerintah di seluruh dunia telah mulai menggunakan informasi yang baru ditemukan untuk membangun warga-sentris, lebih transparan dan mekanisme pemerintah yang lebih akuntabel. Infrastruktur teknologi informasi dan komunikasi yang tersedia bersama dengan kesediaan pemerintah untuk menerapkan *e-governance* telah membawa kesuksesan dalam inisiatif *e-government* di seluruh dunia. Meskipun beberapa negara berkembang telah mengambil langkah-langkah dalam hal ini, mereka sering kali gagal dalam meningkatkan struktur tata kelola dan hasil yang relevan. Di dalam hal ini, ada sejumlah hambatan yang perlu dipahami dan diatasi dengan negara mengembangkan dalam mengejar tujuan *e-government* (As-Saber et al., 2006). Untuk itu ancaman-ancaman ini tidak hanya organisasi di sektor keamanan, tetapi secara keseluruhan, baik ekonomi, sosial maupun humaniter. Hal ini dikarenakan adanya pola keakraban yang dibangun

dalam kerjasama organisasi ini, yang menjadi ancaman bagi negara yang tidak berada di dalam regional tersebut.

Pada sektor strategi, yaitu merebaknya dunia siber sebagai akibat dari meluasnya teknologi informasi. Hal ini menyebabkan sebuah dilema baru bagi negara, yaitu *cyber security* atau keamanan siber. Dengan terintegrasinya seluruh aspek kehidupan melalui teknologi informasi, digitalisasi menjadi sebuah medan baru bagi negara untuk mempertahankan keamanan nasionalnya. Kedaulatan dan otonomi strategis dirasa berisiko saat ini, terancam oleh kekuatan ketegangan internasional yang meningkat, transformasi digital yang mengganggu, dan ledakan pertumbuhan insiden keamanan siber. Kombinasi *Artificial Intelligence* atau kecerdasan buatan dan keamanan siber berada diujung perkembangan ini dan menimbulkan banyak pertanyaan dan dilema etika. Persoalannya bagaimana kita dapat memahami etika *Artifical Intelligence* dan keamanan siber dalam kaitannya dengan kedaulatan dan otonomi strategis. Pendting dalam meganalisis hal ini semestinya diikuti oleh rekomendasi kebijakan, beberapa di antaranya mungkin tampak kontroversial, seperti penggunaan etika secara strategis. Menurut kami dengan refleksi tentang konsep yang mendasari sebagai undangan untuk penelitian lebih lanjut. Dengan artikel ini digarapkan menginspirasi pembuat kebijakan, akademisi dan ahli strategi militer, politik, bisnis dalam pekerjaan mereka, dan menjadi masukan untuk debat public (Timmers, 2019).

Cyber security sebuah negara menunjukkan kesiapannya dalam menghadapi era ini. Digitalisasi aspek-aspek kehidupan tidak melewatkan keamanan sebuah negara. Sebagai salah satu contoh, pernah terjadi kasus penyadapan dari Australia terhadap salah satu Presiden Indonesia. Penyadapan ini dilakukan melalui telepon seluler yang digunakan oleh Presiden Indonesia kala itu, Presiden Susilo Bambang Yudhoyono. Kasus ini bahkan dipublikasi di media-media internasional, yang sayangnya juga, menunjukkan lemahnya pertahanan Indonesia di bidang siber.

Ancaman-ancaman dunia siber tidak terbatas hanya pada penyadapan saja. Spionase, pencurian informasi, bahkan kejahatan lintas negara sekarang dapat dilakukan dimana saja dan kapan saja. Siapa saja dapat menyerang, mencuri informasi, bahkan mampu melakukan kejahatan lintas negara seperti perdagangan gelap. Dari perspektif keamanan nasional, banyak negara-negara berkembang yang belum memiliki pertahanan siber yang memadai. Berangkat dari kasus di Indonesia, masih banyak lagi tindakan-tindakan siber atas negara yang merugikan negara serta memberikan ancaman yang nyata bagi negara.

Gambar 4.1 : Perluasan Studi Keamanan Nasional dalam perspektif politik, hukum dan strategi.

5. Kesimpulan

Implikasi perkembangan industri era 4.0 tidak saja dalam bidang industri dan perdagangan, namun mempengaruhi masalah keamanan. Untuk itu negara diminta mengembangankan persoalan keamanan dari domain negara semata menjadi persoalan bersama, akibatnya negara menyesuaikan dengan merubah kerangkan hukum, politik dan strategi dalam mengahadapi ancaman yang tidak diduga dan belum ada

sebelumnya. Minimnya kemampuan negara-negara berkembang dalam menghadapi tantangan-tantangan baru di era industri 4.0 ini memberikan celah dalam persoalan keamanan nasional lebih. Kemunculan konsep-konsep baru seperti *cyber security* dan *cyber law*, serta pola interaksi negara-negara dunia yang menjadi regionalistik dan berfokus pada *collective security* membuat banyaknya kemungkinan-kemungkinan atas ancaman di level nasional sebuah negara.

Ketidakmampuan menjawab tantangan ini, apabila tidak segera diatasi, mampu membuat sebuah negara tereksploitasi dan terkucilkan, baik dalam level interaksi antar negara hingga ke level individu dalam masyarakat, yang terekspos bahaya dunia siber. Diperlukan sebuah penelitian komprehensif tentang strategi-strategi untuk mengatasi agenda keamanan nasional yang meluasi ini. Penguasaan teknologi informasi yang selalu berkembang menjadi kunci keberhasilan di masa yang akan datang.

Daftar Pustaka

Amaritasari, I. (2015). Keamanan Nasional dalam Konsep dan Standar Internasional. *Jurnal Keamanan Nasional*.

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

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

Barry Buzan, 1991. *People, States and Fear: an Agenda for International Security Studies in the Post-Cold War*. Boulder: Lynne Rienner Publisher.

Barry Buzan & Lenen Hensen. 2009. *The Evolution of International Security Studies.* United Kingdom: Cambridge University Press.

Darmono, 2010. Keamanan Nasional: Sebuah Konsep dan Sistem keamanan Bagi Bangsa

Indonesia, Sekretariat Jendral dewan ketahanan Nasional, Jakarta.

David Mutimer. 1999. *Beyond Strategy: Critical Thinking and the New Security Studies, dalam Contemporary Security and Strategy, Craig A Snyder* (ed), London: Macmillan Press Ltd.

Gultom, R. A. G. (2017). Membangun kemampuan siber dan persandian nasional guna mengantisipasi tantangan keamanan siber di era globalisasi informasi dalam rangka melindungi keutuhan dan kedaulatan NKRI.

Gareth Evans and Bruce Grant, 1992. *Australia's Foreign Relations in The World of 1990's*, Melbourne, Melbourne University Press.

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

Halimatus Sakdiyah. 2010. "*Trafficking perempuan dan anak sebagai isu ancaman keamanan non tradisional bagi Indonesia. Dalam skripsi Mahasiswa UMM jurusan Hubungan Internasional*."

Jack C. Plano dan Ray Olton 1985, The International Relation Dictionary, California ABC-Clio Inc.

James N.Rosenau, 1976, World Politics: An Introduction to International Relations, New York, Free pers.

Julio Tomas Pinto. 2007. Keamanan nasional-Antara Ancaman Internal dan eksternal TIMOR LESTE. Penerbit : ETTIS.

Mas'oed, Mochtar. 1989. Studi Hubungan Internasional, Tingkat Analisis dan Teorisasi. Yogyakarta: Pusat antar Universitas studi Sosial UGM.

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

Perwita, Anak Agung Banyu & Yani, Yanyan A. 2005. Pengantar Ilmu Hubungan Internasional. Bandung: Rosdakarya.

Perwita, Anak Agung Banyu. 2006. *Hakikat Prinsip dan Tujuan Pertahanan-Keamanan Negara, dalam Tim Propatria Institute, Mencari Format Komprehensif Sistem Pertahanan dan Keamanan Negara.* Jakarta: Propatria.

Perwita, Anak Agung Banyu. *Dinamika Keamanan Dalam Hubungan Internasional dan Implikasinya Bagi Indonesia.* Bandung: Universitas Katholik Parahyangan, 2008

Prinsloo, J., Sinha, S., & von Solms, B. (2019). *A review of industry 4.0 manufacturing process security risks. Applied Sciences (Switzerland)*, *9*(23). https://doi.org/10.3390/app9235105

Septa, Albert Alfa. "Ancaman Keamanan Australia Pada Masa Pemerintahan John Howard: 2001-2007." *Jurnal Analisis Hubungan Internasional Vol. 7 No. 2, Mei 2018.*

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

Sujarweni, V. Wiratna. 2014. Metode Penelitian: Lengkap, Praktis, dan Mudah Dipahami. Yogyakarta: Pustaka Baru Press.

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

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