Security and Defence: Ethical and Legal Challenges in The Face of Current Conflict

Michael Christian Budianto, Muhammad Gilang Rasyid, Iqbal Riza Indrawan, dan Samantha Svenska Kendra

Penulis : Frederico Yaniz, Götz Neuneck, Fernanda Navas-Camargo, Carlos Alberto Ardila Castro, Mariano Bartolomé, Bernardino Cortijo Fernández, Pilar Otero, María Méndez Rocasolano, Pablo Moral, Marzanna Farnicka, Juan Cayón Peña, Juan Del Pozo Berenguer, Jordi Regí Rodríguez, Agnieszka Pach-Gurgul, Juliusz Piwowarski, Sonia Boulos, José-Manuel Moreno-Mercado, Adolfo Calatrava-García, dan José-Miguel Calvillo-Cisneros
Penerbit : Springer Nature Switzerland
Tahun : 2022
Halaman : 243

Sudut pandang multidisipliner berbasis etika menjadi pendekatan yang tepat dalam menghadapi konflik di abad ke-21. Coloquio Internacional sobre Cerebro y Agresión International Foundation bersama Antonio de Nebrija University dan didukung oleh Banco de Satander mencanangkan sebuah buku untuk mengumpulkan pendapat ahli dari berbagai bidang keilmuan tentang konflik yang terjadi pada zaman ini. Tema utama dalam buku *Security and Defence: Ethical and Legal Challenges in The Face of Current Conflict* dapat dibagi menjadi dua. Bagian pertama membahas masalah sains dan teknologi, khususnya pada bidang sibernetika. Sementara itu, bagian kedua mendalami permasalahan etis yang dihadapi dalam konflik di zaman ini. Topik-topik yang dibahas dalam buku ini cenderung beragam, sesuai dengan realitas pascamodernisme yang kompleks, kontradiktif, dan bermacam-macam.

Penggunaan ruang angkasa secara damai telah membuka peluang baru untuk kemajuan umat manusia. Satelit buatan pertama, Sputnik 1, diluncurkan ke orbit pada tanggal 14 Oktober 1957 yang diikuti dengan operasi

Badan Penerbangan dan Antariksa Nasional Amerika Serikat (NASA) setahun setelahnya. Sejak saat itu, NASA menjadi salah satu pemain dalam penjelajahan ruang angkasa. Namun, peluang komersialisasi ruang angkasa semakin meningkat seiring berjalannya waktu. Hal ini ditandai dengan munculnya SpaceX, sebuah perusahaan swasta yang mengembangkan program komersial ruang angkasa, sehingga peluncuran pesawat ruang angkasa oleh pihak swasta meningkat. NASA harus beradaptasi dengan privatisasi industri ruang angkasa melalui kerja sama dengan pihak swasta, meskipun menuai kontroversi. Tujuan perusahaan swasta yang umumnya mengejar keuntungan cenderung tidak sejalan dengan lembaga negara yang seharusnya mewakili kepentingan publik. Selama bertahun-tahun, strategi militer Amerika Serikat di luar angkasa cenderung superior. Amerika Serikat memiliki kemampuan untuk mengeksploitasi wilayah di ruang angkasa dan secara selektif tidak mengizinkannya bagi 'musuh' mereka. Seiring berkembangnya zaman, hukum internasional secara jelas membatasi eksplorasi ruang angkasa hanya untuk tujuan damai sehingga melarang penggunaan ruang angkasa untuk tujuan militer. Saat ini, terdapat tanda-tanda bahwa ruang angkasa akan digunakan untuk kepentingan militer, mengingat konsep medan perang yang telah berubah seiring dengan kemajuan teknologi.

Masyarakat modern semakin bergantung pada layanan berbasis ruang angkasa. Oleh karena itu, penggunaan ruang angkasa untuk tujuan damai sangat penting dalam menjaga perdamaian dan keamanan di bumi. Meningkatnya penggunaan ruang angkasa sebagai senjata dan kerentanan satelit menjadi masalah serius yang hanya dapat dibatasi dengan peraturan baru, transparansi yang lebih baik, membangun kepercayaan, dan penetapan standar tertentu. Satelit sifatnya mudah dilacak karena pergerakannya yang secara siklis. Karena strukturnya yang ringan, satelit menjadi sangat rentan

dan dapat dihancurkan pada ketinggian orbit rendah (*Low Earth Orbit*, LEO) terutama oleh sistem pertahanan peluru kendali berbasis darat (*Ballistic Missile Defense*, BMD) milik Amerika Serikat, Rusia, dan Tiongkok, ataupun yang sedang dikembangkan oleh India. Di sisi lain, rivalitas negara-negara telah menjurus pada militerisasi ruang angkasa. Pemerintahan Biden diharapkan akan melakukan upaya serius untuk mendorong peraturan internasional, menetapkan aturan baru untuk ruang angkasa, dan memberikan transparansi yang lebih besar untuk program militer di ruang angkasa.

Perjanjian Luar Angkasa tahun 1967 telah memberikan dasar untuk mengatur penggunaan ruang angkasa di masa depan, namun masih perlu dilengkapi dengan pembangunan kepercayaan, pengendalian senjata, dan implementasi yang lebih baik dari standar yang telah lama diterima. Perjanjian ini adalah perjanjian multilateral pertama yang mengikat dan dengan demikian memperluas Piagam Perserikatan Bangsa-Bangsa (PBB) ke ruang angkasa. Dalam pembukaannya, perjanjian ini menekankan "kepentingan bersama seluruh umat manusia dalam eksplorasi progresif dan penggunaan ruang angkasa untuk tujuan damai." Oleh karena itu, ruang angkasa adalah ruang bersama yang berdaulat, yang penggunaannya harus "demi kepentingan semua negara" dan "umat manusia secara keseluruhan." Meskipun pengendalian senjata di ruang angkasa harus didasarkan pada prinsip-prinsip hukum ruang angkasa internasional, pengaturan pengendalian senjata tambahan di antara negara-negara ruang angkasa terkemuka di dunia dapat membantu mencegah tindakan perang di ruang angkasa.

Selain terkait penggunaan ruang angkasa, globalisasi juga membawa banyak tantangan ke dalam agenda domestik yang berkaitan dengan strategi

keamanan dan pertahanan nasional. Digitalisasi informasi, data, dan proses menghadirkan banyak peluang sekaligus ancaman. Salah satu tantangan utama adalah pemanfaatan secara bertanggung jawab pada data yang dikumpulkan. Untuk mencegah kebocoran informasi, tidak hanya dibutuhkan mesin yang kuat, tetapi penting juga untuk mengetahui mengapa suatu data diperlukan, bagaimana data tersebut dapat digunakan secara positif dan negatif, serta bagaimana data tersebut dapat membantu negara untuk beralih ke otomatisasi aktivitas tertentu. Kecerdasan buatan (*artificial intelligence*, AI) akan terus ada, sehingga terdapat ancaman bahwa akan muncul mesin yang dapat melampaui kemampuan manusia. Oleh karena itu, sumber daya manusia adalah elemen terpenting dalam menetapkan pedoman penggunaan data yang wajar dan bertanggung jawab untuk mengenali ancaman keamanan yang berkaitan dengan AI. Sebagai contoh, Kolombia biasanya disorot karena banyaknya masalah dan konflik bersenjata. Namun, dengan banyaknya tantangan yang masih dihadapi, komunitas internasional mulai mengakui Kolombia sebagai negara Amerika Latin pertama yang menerapkan kebijakan publik terkait penggunaan AI dalam proses pelayanan publik. Ekspansi teknologi dan interkoneksi menyebabkan perubahan struktur hubungan antara sipil dan angkatan bersenjata. Dalam hal ini, penggunaan angkatan bersenjata harus disesuaikan dengan kondisi peperangan yang dinamis di era globalisasi.

Selama dekade kedua abad ini, masalah keamanan di dunia maya semakin penting. Dunia maya telah menjadi tempat terjadinya berbagai risiko dan ancaman dengan jenis yang berbeda. Dengan demikian, keamanan siber cenderung memiliki intensitas dan tingkat heterogenitas yang tinggi. Keberadaan kelompok-kelompok tipe ancaman tingkat lanjut yang berkepanjangan (*advanced persistent threat,* APT) yang terkadang bertindak secara otonom, atau di lain waktu menjadi proksi negara, berkontribusi pada

kompleksitas ini. Meskipun kelompok APT umumnya berada di bawah label aktivitas spionase siber, pengejaran keuntungan finansial melalui tindakan pemerasan, seperti pada WannaCry dan NotPetya, juga sesuai dengan profil kejahatan siber. Selain negara dan kelompok tipe APT, pihak yang terlibat dalam peristiwa keamanan siber mencakup gerakan *hacktivist* (Anonymous) dan orang dalam (Wikileaks) dengan kapasitas yang luar biasa untuk menghasilkan kerusakan. Target pelaku adalah perusahaan negara (Stuxnet, Black Energy, Wikileaks), swasta (Sony Pictures, Anonymous), campuran (WannaCry, NotPetya, Anonymous), dan bahkan masyarakat sipil sebagai aktor, seperti dalam kasus Cambridge Analytica dan Russiagate. Alat dan teknik yang digunakan oleh para pelaku serangan siber cenderung beragam, seperti *malware*, virus (misalnya, Stuxnet dan Black Energy), atau *worm* (misalnya, WannaCry dan NotPetya). Selain itu, Anonymous sering menggunakan teknik *Distributed Denial of Service* (DDoS) serta *phishing* yang telah digunakan setidaknya pada tiga kesempatan, yakni Black Energy, Russiagate, dan Sony Pictures.

Semua kompleksitas ini menegaskan bahwa keamanan siber menempati posisi istimewa dalam agenda keamanan internasional kontemporer. Dapat diperkirakan bahwa hierarki keamanan siber akan cenderung meningkat dalam jangka pendek dan menengah akibat kemajuan teknologi yang berdampak pada dinamika di dunia maya. Namun, hal ini tidak tercermin dalam konsensus yang dicapai di tingkat multilateral. Tidak diragukan lagi bahwa penandatanganan Konvensi Keamanan Siber, dengan dukungan kuat dari negara-negara utama, akan memberikan kontribusi untuk penanganan yang lebih efektif terhadap masalah ini. Namun, perbedaan mendasar antara demokrasi barat dengan Rusia dan Tiongkok tetap menjadi hambatan. Peningkatan mekanisme tata kelola di berbagai aspek keamanan siber dalam skala global juga akan memberikan dampak

positif yang kuat di lapangan. Dalam skenario yang ideal, mekanisme ini harus secara aktif melibatkan berbagai pemangku kepentingan publik, swasta, dan masyarakat sipil.

Terdapat sejumlah faktor yang memengaruhi risiko di dunia maya. Pertama, *the cloud*, sebuah sistem keamanan cadangan untuk melakukan penyimpanan data di internet yang dapat diakses melalui koneksi jaringan publik dan pribadi. Kedua, *Internet of Things* (IoT), sebuah perkembangan teknologi yang memungkinkan perangkat lunak maupun perangkat keras untuk mengelola atau bahkan dikelola dari jarak jauh atau mandiri selama masih terhubung ke internet. Contoh nyata dari IoT yang komprehensif adalah sistem robot (industri 4.0) dan peralatan fisik dengan bantuan terprogram lainnya yang digunakan untuk mempermudah aktivitas manusia. Ketiga, 5G dan 5G-DIVE, sistem teknologi seluler nirkabel yang menawarkan kecepatan lebih tinggi untuk aktivitas unggah dan unduh, serta koneksi yang lebih konsisten untuk mengakses internet dibandingkan dengan jaringan pendahulunya. Ketiga kemajuan teknologi tersebut bekerja secara berkesinambungan. Pada saat yang sama, mereka dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab sebagai titik masuk ke dalam sistem organisasi dan pemerintahan, yakni untuk mengendalikan sistem maupun aktivitas kewarganegaraan dan pertahanan. Dalam praktiknya, teknik yang paling sering terjadi dalam kejahatan dunia maya adalah yang terkait dengan pemerasan *ransomware* (jenis *malware* yang mencegah pengguna dari mengakses komputernya, termasuk data yang disimpan di dalamnya. Komputer itu sendiri mungkin terkunci, tetapi data di dalamnya mungkin dicuri, dihapus, atau dienkripsi) dan *phishing* (serangan yang bertujuan untuk mencuri uang, atau identitas, dengan membuat pengguna mengungkapkan informasi pribadi—seperti nomor kartu kredit, informasi bank, atau kata sandi—melalui situs web yang berpura-pura sah). Perangkat apa pun dapat

disusupi, termasuk kendaraan, rumah, perusahaan, peralatan pertahanan atau serangan, serta bahkan elemen dalam sistem *smart city* seperti sistem distribusi dan penyimpanan air, energi, kontrol lalu lintas, dan armada.

Upaya untuk memberantas kejahatan dunia maya sudah dilakukan oleh sejumlah negara. Spanyol, misalnya, memiliki peraturan yang berlaku terkait keamanan nasional yang mencakup sebagian atau keseluruhan aspek keamanan dan kejahatan dunia maya. Salah satu peraturannya adalah Ley de Protección de Datos Personales Y Garantías de los Derechos Digitales atau Undang-Undang tentang Perlindungan Data Pribadi dan Jaminan Hak Digital. Pada tingkat wilayah Eropa juga memiliki sejumlah regulasi termasuk Konvensi Kejahatan Dunia Maya Budapest dan Dekrit No. 2016/1148 tentang Langkah-Langkah Keamanan dalam Jaringan dan Sistem Informasi Uni Eropa. Kesepakatan secara global masih belum ada walaupun berbagai peraturan sudah dibuat oleh masing-masing negara.

Meningkatnya serangan dunia maya mengharuskan organisasi untuk memiliki kepatuhan dunia maya atau *cybercompliance*. Sistem kepatuhan dunia maya tersebut mencakup gambaran risiko di setiap organisasi yang dapat menawarkan kemampuan bagi karyawan untuk selalu waspada terhadap kemungkinan terjadinya tindakan ilegal. Penting bagi organisasi untuk memahami langkah-langkah deteksi dini tindakan peretasan dan serangan dunia maya, seperti mendeteksi pencurian data dan pemantauan perlindungan data pribadi, mengembangkan sistem pendeteksi serangan, pelanggaran komunikasi, klasifikasi informasi berikut penerapan perlindungannya, dan analisis individu yang terlibat dalam bisnis (dengan bantuan sistem intelijen dunia maya), serta memiliki kontrol organisasi dan teknologi yang cermat.

Berbeda dengan bagian pertama yang cenderung membahas tentang perkembangan sains dan teknologi terhadap permasalahan keamanan dan pertahanan secara berkaitan, bagian kedua buku *Security and Defence: Ethical and Legal Challenges in The Face of Current Conflict* lebih mendalami tentang hubungan konflik kontemporer dengan permasalahan etika yang dihadapi saat ini. Tema yang diusung jauh lebih beragam ketimbang bagian pertama. Namun, semua tulisan dalam bagian ini memiliki keterkaitan dampak terhadap keamanan dan stabilitas negara.

Pembahasan pertama di bagian kedua buku berfokus pada pendekatan psikologi positif dengan berargumen bahwa kekerasan tidak hanya berasal dari faktor biologis saja, tetapi juga etika dan norma dari lingkungan yang dimiliki. Berkat perkembangan ilmu saraf dan psikologi, saat ini dapat dipahami mengapa manusia mengalami stres, trauma, dan bagaimana lingkungan mempengaruhi mereka seperti rasa tidak aman, keberadaan teman, hingga otoritas penguasa. Faktor-faktor ini berpengaruh terhadap perilaku etika seseorang kepada norma-norma yang ada.

Pengetahuan akan hal tersebut telah membuka ruang untuk memahami, mengatasi, mengurangi, dan membalikkan respons seseorang terhadap kenyataan yang dapat berdampak negatif. Melalui pendekatan psikologi positif yang bertujuan untuk menganggap individu sebagai makhluk yang kreatif dan produktif, menikmati hidup, dan dapat mengatasi kesulitan, perspektif ini melihat perlunya kesejahteraan sosial bagi individu dan masyarakat dari sisi kapabilitas mental, sosial, dan material. Kapabilitas mental merupakan tujuan dari individu dan sudut pandang mereka terhadap dunia. Kapabilitas sosial berkaitan dengan lingkungan seorang individu. Sementara beberapa contoh dari kapabilitas material meliputi kemampuan ekonomi, militer, dan infrastruktur. Untuk mendukung hal tersebut,

dibutuhkannya stimulasi dengan mengintegrasikan ilmu, teknologi dan produksi di bidang pendidikan. Melalui pendekatan ini, akan tercipta lingkungan yang mendukung peningkatan keamanan, baik individu, masyarakat, maupun negara pada masa mendatang.

Pembahasan kedua lebih bersifat tradisional mengenai permasalahan teritorial yang dikaitkan dengan aspek etika dan hukum di Spanyol. Konflik teritorial merupakan masalah klasik di bidang pertahanan dan keamanan. Tujuan utama dari negara adalah untuk memastikan *common good* dari semua kelompok di dalam negeri terpenuhi. Dalam konteks Spanyol, mereka melakukan delegasi kekuasaan kepada komunitas otonom sesuai dengan konstitusi Spanyol 1978. Hal ini dilakukan dengan tujuan untuk meningkatkan efektivitas, meningkatkan solidaritas teritorial, memberikan kekuasaan pada rakyat, dan menghargai perbedaan historis. Spanyol dapat dikatakan merupakan negara kesatuan dengan desentralisasi yang tinggi. Namun, keberadaan dari desentralisasi ini menjadi suatu ancaman ketika ada tendensi separatisme yang dapat mengganggu integritas teritorial negara. Desentralisasi tersebut meningkatkan rasa perbedaan di dalam suatu negara yang menjadi bahan bakar separatisme. Untuk mengatasi hal tersebut, keberadaan dari Mahkamah Konstitusi menjadi institusi yang penting bagi pemerintah pusat untuk merepresi kekuatan politik komunitas otonom secara legal. Selain itu, negara harus memberlakukan secara rutin upaya meningkatkan rasa persatuan dari berbagai komunitas otonom.

Pembahasan ketiga berkaitan dengan penggunaan sistem nirawak yang didefinisikan sebagai kendaraan udara tanpa pilot, dengan elemen kuncinya adalah otomatisasi yang membuatnya dapat melakukan tugas tanpa intervensi manusia. Melalui hal tersebut, seseorang dapat memerintahkan sistem nirawak untuk beraksi dari jarak ribuan kilometer. Hal

ini menimbulkan dilema etika terhadap penggunaan sistem nirawak. Penggunaan sistem nirawak dalam suatu operasi dari jauh ini harus benar-benar dapat dijustifikasi. Di sisi lain, keberadaan dari sistem nirawak akan meningkatkan akurasi yang dapat meminimalkan penderitaan korban sesuai dengan Hukum Humaniter Internasional. Pada dasarnya, penggunaan dari sistem nirawak ini membawa implikasi terhadap etika dan hukum.

Pembahasan keempat mengevaluasi tantangan dan permasalahan etika yang dihadapi Amerika Serikat, Italia, Spanyol, dan Tiongkok dalam menghadapi pandemi COVID-19. Terdapat tiga klasifikasi penanganan pandemi, yakni (1) cepat dan efektif, (2) lunak, dan (3) lambat. Berdasarkan hal tersebut, Tiongkok ada pada klasifikasi cepat dan efektif, sedangkan Italia dan Spanyol berada di lunak, dan Amerika Serikat pada kategori lambat. Perbedaan respons keempat negara ini dapat ditunjukkan dari jumlah kasus COVID-19. Tiongkok memiliki jumlah kasus yang sangat sedikit dibandingkan dengan Italia, Spanyol, maupun Amerika Serikat. Namun, respons Tiongkok nyatanya membawa persoalan etika. Penanganan pandemi COVID-19 menunjukkan kontradiksi antara keamanan dan kebebasan. Hal ini terutama sangat penting di negara-negara demokrasi ketimbang oritarian seperti Tiongkok. Penggunaan langkah seperti *lockdown,* karantina, dan pengumpulan data tanpa izin menjadi perdebatan panas di sana. Di satu sisi, mereka harus mengedepankan kepentingan bersama dengan mencegah penyebaran COVID-19. Di sisi lain, mereka juga harus menghormati hak-hak yang dimiliki oleh individu. Dalam menghadapi dilema ini, otoritas kesehatan harus mampu memberikan justifikasi terkait kewajiban etika mereka dalam melindungi masyarakat dari ancaman kesehatan.

Terdapat pembahasan di bagian lain pada buku yang juga mengenai dampak penanganan pandemi COVID-19. *Lockdown*, pembatasan

pergerakan, serta upaya untuk memerangi misinformasi terkait pandemi memberikan dampak buruk pada kapasitas media dan masyarakat umum dalam memperoleh informasi yang akurat. Sejumlah pemerintah nyatanya mengeksploitasi pandemi COVID-19 untuk menekan kebebasan berekspresi, dengan maksud untuk membungkam perbedaan pendapat publik. Jika melihat situasi di Spanyol, pemerintah pusat maupun daerahnya justru sama-sama telah memenuhi kewajiban mereka di bawah hukum internasional untuk menghormati dan memastikan kebebasan berbicara selama pandemi. Berdasarkan laporan Ekspresi Global tahun 2021, yang melacak kebebasan berekspresi di 161 negara, Eropa adalah rumah bagi beberapa negara demokrasi paling mapan di dunia dan negara-negara dengan skor tertinggi dalam hal kebebasan berbicara termasuk pada saat darurat kesehatan global. Kebebasan berbicara menjadi penting, mengingat negara-negara dengan catatan kuat tentang kebebasan gagal menghadapi pandemi sambil sepenuhnya menghormati standar hak asasi manusia internasional tentang kebebasan berbicara. Laporan tersebut mengidentifikasi pelanggaran standar hak asasi manusia internasional dalam kaitannya dengan kebebasan berbicara dan kebebasan informasi yang terjadi di Spanyol pada tahun 2020. Pembahasannya termasuk apakah pihak berwenang Spanyol telah memenuhi kewajiban mereka di bawah hukum internasional untuk menghormati dan memastikan kebebasan berbicara selama pandemi. Pembatasan yang diberlakukan selama pandemi berisiko merugikan pelaksanaan pidato politik, bahkan setelah pandemi berakhir. Kebebasan berbicara telah digambarkan sebagai landasan dari semua hak asasi manusia dan dilindungi oleh instrumen hak asasi manusia internasional. Pembatasan sebenarnya bisa terjadi, namun hanya dapat dilakukan apabila didasarkan pada hukum untuk (1) menghormati hak atau reputasi orang lain, maupun (2) melindungi keamanan nasional, ketertiban umum, kesehatan, atau moral publik.

Pembahasan selanjutnya menyoroti tantangan dari serikat energi. Saat ini, lebih dari setengah energi yang digunakan di Uni Eropa berasal dari impor. Selain daya saing dan perlindungan lingkungan, ketahanan energi menjadi salah satu dari tiga prioritas kebijakan energi Uni Eropa. Guna melancarkan kebijakan energi tersebut, pada tanggal 25 Februari 2015, Komisi Eropa menyetujui dokumen terkait pembentukan Serikat Energi. Proyek itu bertujuan untuk memberikan keamanan energi, terutama bagi negara-negara yang bergantung pada pasokan energi hanya dari satu sumber. Serikat Energi ini mengasumsikan bahwa integrasi lebih lanjut dalam Uni Eropa akan menyebabkan evolusi sikap negara-negara anggota yang berorientasi pada kepentingan seluruh Uni Eropa secara keseluruhan dan keamanan energi bersama. Definisi yang diberikan oleh Komisi Eropa menunjukkan bahwa keamanan energi Uni Eropa dapat dipahami sebagai akses tak terputus ke energi setiap saat, dalam jumlah yang cukup, dan dengan harga yang wajar.

Terdapat pembahasan berikutnya yang menyorot bagaimana migrasi diposisikan sebagai masalah keamanan yang multidimensi. Salah satu turunan dari perluasan konsep keamanan, yang terbukti dalam kasus kebijakan migrasi, adalah proses sekuritisasi. Konsep ini berasal dari pendekatan konstruktivis untuk ilmu hubungan internasional dan keamanan, khususnya Sekolah Kopenhagen. Sekuritisasi menjelaskan bagaimana masalah politik yang didefinisikan oleh pembentukan kebijakan publik berakhir di bidang keamanan karena tindak aktor utama. Akibatnya, masalah migrasi dimasukkan ke dalam agenda keamanan pemerintah dan organisasi internasional. Sebagai contohnya, pemerintah sosialis menciptakan kebijakan migrasi dalam konteks krisis Cayuco. Sejak itu, kebijakan migrasi telah mengalami proses politisasi dan sekuritisasi. Secara tradisional, sekolah teoritis klasik ilmu hubungan internasional sangat mementingkan ancaman dari

negara lain. Namun, mengingat ketergantungan yang kini semakin kompleks, agenda hubungan internasional terdiri dari berbagai masalah tanpa hierarki yang jelas. Hal ini berarti bahwa keamanan militer tidak lagi mendominasi agenda, sehingga studi terkini tentang migrasi internasional masuk dalam studi keamanan. Selain itu, negara-negara dan organisasi internasional memperkenalkan perspektif ini dalam strategi keamanan internal dan eksternal mereka. Dalam kebijakan migrasi, proses sekuritisasi adalah salah satu perpanjangan dari konsep keamanan. Proses sekuritisasi memungkinkan elite untuk mengendalikan masalah ini karena mereka telah membangun persepsi negatif tentang migrasi. Di Eropa dan Amerika Serikat, politisasi kebijakan imigrasi telah menjadi elemen dalam proses sekuritisasi. Dapat disimpulkan bahwa kebijakan migrasi harus menyeimbangkan masalah keamanan, kebijakan penerimaan dan integrasi, serta penghormatan terhadap hak asasi manusia.

Pada akhirnya, dapat disimpulkan bahwa bagian pertama buku ini membahas permasalahan di ruang angkasa, termasuk penggunaan ruang angkasa oleh entitas publik maupun privat serta militerisasi yang semakin meningkat. Selanjutnya, bagian ini juga mengkaji permasalahan keamanan yang terjadi di abad ke 21, khususnya keamanan siber dan penggunaan teknologi. Dalam hal ini, terdapat ancaman keamanan siber bagi entitas publik dan privat, adanya permasalahan hak asasi manusia yang lahir dari penggunaan teknologi seperti kecerdasan buatan dan *big data*, serta ancaman misinformasi bagi keamanan nasional. Bagian kedua buku membahas permasalahan yang beragam, mulai dari hubungan psikologi manusia dan konflik, alasan filosofis dari meningkatnya konflik dan kesatuan wilayah di beberapa negara Eropa, operasi militer serta kaitannya dengan hukum humaniter manusia dan hak asasi manusia, dampak ekonomi dan pembangunan dari pandemi COVID-19, serta ancaman ketahanan energi.

Buku ini diakhiri dengan dua bab berkaitan dengan tantangan yang signifikan bagi masyarakat, yaitu menjaga kebebasan berekspresi di masa-masa sulit.