# PERANG TANPA NEGARA

## INTELIJEN DAN TERORISME DALAM ARSITEKTUR KEAMANAN INTERNASIONAL

PROF. ANGEL DAMAYANTI
DR. PRATAMA PERSADHA

**November 2025**

# PERANG TANPA NEGARA

## INTELIJEN DAN TERORISME DALAM ARSITEKTUR KEAMANAN INTERNASIONAL


Penulis : Prof. Angel Damayanti, Ph.D
Dr. Pratama Persadha
Editor : Dahniar Wisnu
Desainer Cover : Dr. Pratama Persadha



Diterbitkan oleh:
**CISSReC - Yayasan Lembaga Riset Siber Indonesia**
Jl. Moh. Kahfi 1 No.88 D8 RT.08/RW.04, Jagakarsa,
Kec. Jagakarsa, Jakarta Selatan, DKI, 12620
Telp: 021 77215999
info@cissrec.org

Anggota IKAPI No: 651/DKI/2025



ISBN: 978-634-7468-20-8
Cetakan pertama, 2025

# DAFTAR ISI

# KATA PENGANTAR

Dalam dekade terakhir, dunia tempat kita hidup telah mengalami perubahan yang dramatis dan menantang dalam aspek keamanan. Di tengah era informasi, di mana perkembangan teknologi melaju tanpa henti, ancaman datang bukan hanya dari aktor negara, tetapi juga dari mereka yang beroperasi dalam bayang-bayang dan lintas negara seperti kelompok teroris, jaringan kriminal, dan ancaman siber. Buku ini, "Perang Tanpa Negara: Intelijen dan Terorisme dalam Arsitektur Keamanan Internasional," bertujuan untuk menjelajahi dunia yang kompleks dan dinamis ini, serta memberikan pemahaman yang dapat diandalkan mengenai mekanisme yang mengaturnya.

Penulisan buku ini didorong oleh kebutuhan yang mendesak untuk memahami bagaimana aktor-aktor non-negara dan digital telah mengubah lanskap keamanan global. Virus digital dapat melumpuhkan negara, ancaman tanpa bendera dapat menyebabkan ketakutan yang meresap, dan di tengah semua itu, pertarungan intelijen menjadi garis depan baru dalam mempertahankan kedaulatan dan keamanan. Urgensi ini membuat buku ini relevan baik bagi praktisi di sektor keamanan, mahasiswa, maupun masyarakat umum yang penasaran mengenai tantangan dunia modern yang tidak kasatmata.

Dalam struktur yang sistematis, buku ini menyusun materi dari dinamika aktor non-negara hingga evolusi terorisme digital, serta memainkan peran intelijen global dalam menjaga dan sekaligus mengganggu tatanan dunia. Mulai dari analisis tentang dunia baru dengan musuh tak kasatmata, buku ini mengupas ideologi teroris yang berkembang dengan pesat, peran intelijen dalam mempengaruhi hegemoni global, hingga tantangan perang siber dan kontribusi sektor swasta dalam keamanan internasional. Setiap bab dirancang untuk memberi pembaca wawasan komprehensif dan kritis mengenai bentuk ancaman dan strategi penanganannya, membekali pembaca dengan pengetahuan yang diperlukan untuk mendekati masalah-masalah ini secara bijak.

Penulisan buku ini tidak akan mungkin tanpa kontribusi luar biasa dari sejumlah orang dan entitas yang mendukung proses pengembangan ini. Kami ingin mengucapkan terima kasih kepada para peneliti, analis intelijen, dan praktisi keamanan yang telah berbagi wawasan dan pengalaman mereka. Terima kasih juga kami haturkan kepada keluarga dan teman-teman yang memberikan sokongan emosional dan intelektual selama proses penulisan. Tak kalah pentingnya adalah dukungan dari para editor dan penerbit yang telah bekerja keras memastikan penyampaian buku ini dapat dinikmati banyak kalangan.

Harapan kami, setelah membaca buku ini, para pembaca dapat memiliki pemahaman yang lebih mendalam tentang tantangan keamanan abad ke-21 dan lebih siap untuk berperan aktif dalam menciptakan solusi yang konstruktif. Semoga buku ini menginspirasi diskusi yang produktif dan kolaborasi yang lebih kuat di berbagai lini untuk menghadapi ancaman yang, meski tidak kasatmata, nyata dan berbahaya bagi tatanan dunia kita.

Selamat membaca dan mari bersama-sama membangun dunia yang lebih aman dan damai.



# BAB 1

# DUNIA BARU DAN MUSUH TAK KASATMATA

Dalam dekade terakhir, benua kehidupan kita telah mengalami pergeseran paradigmatis yang mengubah cara kita memandang keamanan dan ancaman. Dunia baru yang kita hadapi bukan lagi didominasi oleh batas-batas teritorial negara, melainkan oleh batas-batas maya yang merekat erat dengan arus globalisasi. Di tengah revolusi digital dan era informasi, arsitektur keamanan internasional menghadapi tantangan yang tak pernah terbayangkan sebelumnya. Konsepsi tradisional mengenai peperangan dan keamanan perlu dirombak secara fundamental untuk menyesuaikan diri dengan realitas yang semakin kompleks dan dinamis.

Terorisme, yang dahulu mungkin dianggap sebagai ancaman lokal atau terbatas pada wilayah tertentu, kini menjelma menjadi ancaman global sebuah bahaya laten yang melintasi batas-batas negara, melampaui sekat-sekat kultural, dan melebur dalam jaringan informasi global. Di sinilah peran intelijen dan adaptasi strategi keamanan mendapatkan ujiannya yang paling berat. Musuh yang dihadapi bersembunyi di balik wajah yang tak kasatmata, mereka adalah entitas tanpa negara yang mampu menyamarkan kehadirannya dalam kabut kerumitan teknologi modern.

Keberhasilan tindakan kontra-terorisme dan upaya melindungi warganegara dari ancaman ini tidak hanya bergantung pada kekuatan militer dan diplomasi, tetapi juga pada kemampuan sistem keamanan untuk mengumpulkan, menganalisis, dan menyebarluaskan informasi yang tepat waktu dan akurat. Intelijen memainkan peran kunci sebagai radar dalam mengidentifikasi ancaman yang tersembunyi di balik permukaan merekayasa data untuk mengungkap pola dan tanda-tanda yang dapat mencegah serangan sebelum terlambat.

Namun, tantangan sesungguhnya adalah bagaimana menyusun strategi yang tidak hanya reaktif tetapi juga proaktif dalam menghadapi kelompok-kelompok yang mengembangkan taktik dan metode baru untuk menyerang. Di sinilah teknologi canggih, seperti kecerdasan buatan dan analisis data besar, menjadi alat vital bagi aparat keamanan untuk bertahan dalam perang asimetris yang berlangsung di dunia maya. Dalam dunia baru ini, kolaborasi internasional menjadi keniscayaan.

Negara-negara harus bersatu dalam melawan ancaman bersama yang tidak mengenal paspor atau batas negara. Hanya dengan sinergi antara komunitas global, baik melalui pertukaran intelijen maupun dengan menetapkan standar keamanan kolektif, kita dapat menghadapi musuh yang tidak terlihat ini.

Selain itu, ada kebutuhan mendesak untuk menggali lebih dalam pada akar permasalahan yang mendorong radikalisasi dan membentuk narasi alternatif yang membangun kedamaian dan toleransi. Pendidikan, dialog antar-agama, dan kebijakan yang inklusif adalah beberapa dari banyak alat yang dapat mengurangi daya tarik ideologi ekstremisme.

Perang tanpa negara menuntut pendekatan yang menyeluruh dan holistik dalam arsitektur keamanan internasional. Merebut kembali rasa aman bukanlah tentang menghancurkan musuh secara fisik, tetapi tentang memenangkan hati dan pikiran orang-orang. Kita perlu memasuki dunia baru ini dengan pemahaman yang lebih dalam tentang musuh tak kasatmata di tengah kita, dan dengan kebulatan tekad untuk melindungi dunia yang semakin terhubung ini dari kekacauan dan ketakutan. Keberanian dan kecerdasan kita dalam menyusun strategi keamanan akan menentukan masa depan keamanan dan perdamaian di dunia modern ini.

## 1.1 Ketidakpastian dalam Arsitektur Global

Era pasca-Perang Dingin telah mengantarkan kita ke dalam lanskap global yang ditandai oleh ketidakpastian multidimensional. Di bawah bayang-bayang keberhasilan menghadapi persaingan bipolar yang mengadu Uni Soviet (atau Rusia sekarang) dan Amerika Serikat (AS), dunia memasuki fase baru di mana aktor-aktor non-negara mengemuka sebagai ancaman yang nyata dan tak terduga (Kaldor, 2012). Ketidakpastian ini difasilitasi oleh kemajuan teknologi, globalisasi, dan kemudahan informasi, menjadikan dunia semakin terkoneksi namun serentak terpecah dalam kerangka keamanan internasional yang retak (Buzan & Waever, 2003; Freedman, 2006).

Dalam bab ini, kita akan menjelajahi dinamika dunia baru yang muncul dari reruntuhan tatanan lama. Sebelumnya, keamanan

internasional banyak dipahami melalui lensa negara-bangsa dan militerisme konvensional. Namun, kini ancaman datang dari berbagai arah yang tak selalu diakui oleh batas geografis atau diidentifikasi dengan mudah. Dalam konteks ini, musuh-musuh yang tak kasatmata terorisme, jaringan kriminal transnasional, dan potensi serangan siber menuntut kita melakukan redefinisi tentang keamanan.

Begitu Perang Dingin berakhir, perhatian dunia secara pragmatis beralih dari pertarungan ideologis menuju pencarian kesetimbangan baru. Demokrasi berkembang pesat di banyak bagian dunia (Huntington, 1991), namun bukan tanpa tantangan (Diamond, 2015). Ketika tembok Berlin roboh dan sangkar batas ideologi mulai memudar, muncul pula kekosongan yang mengizinkan berbagai ideologi ekstrem untuk merebut ceruk pengaruhnya sendiri. Ide-ide ini sering dibungkus dengan retorika yang memikat, menjanjikan perubahan melalui cara-cara yang menghindari pengawasan otoritas formal negara.

Pergerakan ini semakin intensif dengan kehadiran internet dan kemajuan teknologi komunikasi. Internet, sebagai sebuah ekosistem global, menawarkan kemungkinan tak terbatas bagi ideologi dan propaganda tersebar dengan cepat ke penjuru dunia. Platform digital menjadi sarang bagi aktor aktif-imajiner baru, membudayakan jaringan kompleks yang memperdebatkan setiap elemen dari kehidupan sehari-hari dan hubungan antar negara. Di sinilah kesenjangan antara negara dan entitas non-negara menjadi sangat mencolok.

Dalam bab ini, perhatian khusus diberikan pada modus operandi entitas non-negara dalam mencapai tujuan mereka. Ketidakpastian yang mencakup bagaimana serangan teror bisa terjadi, siapa yang berada di belakangnya, dan motivasi apa yang mendorong mereka, merupakan tantangan besar bagi komunitas intelijen dan badan keamanan di seluruh dunia. Strategi konvensional dalam menangani ancaman jenis ini sering menemukan batasannya. Pembinaan dalam jaringan rahasia, kemudahan bergerak, serta kemampuan menyusup dan bersembunyi di antara warga sipil adalah bagian dari kompleksitas yang dibawa terorisme internasional ke panggung global.

Para analis keamanan internasional sering menyoroti transformasi dari perang konvensional menuju apa yang disebut "peperangan asimetris" (Buffaloe, 2006). Ini adalah taktik dimana kelompok kecil namun sangat militan, terorganisir dan termotivasi dapat menghadapi kekuatan yang jauh lebih besar melalui strategi yang cerdik dan penggunaan teknologi secara kreatif (Record, 2007; Boot, 2013; Arquilla & Ronfeldt, 2001; Johnson & Tierney, 2011). Serangan bom bunuh diri, penculikan, sabotase infrastruktur kritis, hingga serangan siber adalah metode yang kerap digunakan untuk melumpuhkan lawan yang konvensional lebih kuat (Clarke & Knake, 2010; Singer & Friedman, 2014; Kello, 2017).

Namun, lebih dari sekadar ancaman fisik, kehadiran aktor non-negara ini menjulurkan tantangan di ranah psikologis dan ideologis. Di zaman ketika informasi bergerak secepat cahaya, taktik penyebaran ketakutan dan propaganda jauh lebih efektif daripada sebelumnya. Narasi teror mampu menciptakan rasa tidak aman dan ketidakpercayaan yang menggerogoti tatanan sosial, memecah belah komunitas, dan mengganggu kestabilan politik serta ekonomi (Awan, 2011; Ingram, 2016). Ini adalah "peperangan budaya" yang dirancang untuk mengganggu cara berpikir masyarakat, mengaburkan batas antara kenyataan dan distorsi (Seib & Janbek, 2011).

Salah satu aspek yang paling membingungkan dari ancaman ini adalah ketidakstabilan definisi dan batasan terorisme itu sendiri (Hoffman, 2006). Berbeda perspektif antara satu negara dengan lainnya, terorisme dapat dilihat sebagai tindakan kriminal yang memerlukan pendekatan penegakan hukum; sementara bagi yang lain, ia merupakan tindakan perang yang memerlukan respons militer. Ketidaksepakatan mengenai definisi ini menambah lapisan kompleksitas dalam upaya kolektif untuk melawan musuh tak kasatmata yang secara efektif dapat beroperasi di ruang-ruang abu-abu, antara legalitas dan kekacauan.

Sementara ulah musuh tak kasatmata ini berdampak langsung terhadap hubungan internasional dan arsitektur keamanan global, negara-negara di belahan dunia ini menunjukkan respon yang berbeda-beda. Beberapa memilih pendekatan militeristik dengan memperkuat

perangkat keras pertahanan dan menetapkan kebijakan kontra-terorisme yang ketat seperti AS, Malaysia, Filipina dan Thailand (Pradnyana, 2022). Namun, tak jarang kebijakan ini mendapat kritik karena sering merambah pada hak asasi manusia, menciptakan budaya ketakutan, dan melahirkan efek bola salju pada radikalisasi lebih lanjut.

Sebaliknya, ada pula upaya yang lebih terukur dengan menggali akar penyebab terorisme dan fokus pada solusi diplomatis serta kebijakan *soft-power*, seperti Indonesia melalui Badan Nasional Penanggulangan Terorisme (BNPT). Pendekatan ini menggencarkan pekerjaan yang berupaya menghapus kebencian dan pembentukan identitas musuh, menggantinya dengan dialog antar budaya serta inisiasi program-program deradikalisasi yang bertujuan mengubah pola pikir para pelaku kekerasan ekstrem.

Namun demikian, upaya ini tidaklah mudah. Kegagalan intelijen, birokrasi, serta kebijakan multi-dimensi seringkali menciptakan hambatan bagi respons efektif. Di sinilah letak tantangan utama bagi komunitas internasional: mengintegrasikan berbagai pendekatan dalam satu visi yang koheren dan strategis untuk mengatasi ancaman terorisme serta memastikan keamanan bersama.

Bab ini juga menelaah bagaimana perkembangan teknologi dan perpindahan data besar menjadi pisau bermata dua. Data dan analitik yang canggih memungkinkan deteksi dini dan penangkapan ancaman, namun juga meningkatkan risiko terhadap privasi individu dan kebebasan sipil. Implikasi dari pengawasan massal, peretasan privasi, dan manipulasi informasi digital menciptakan dilema etis yang menguji batas dari masyarakat bebas.

Keberhasilan dalam menangani musuh tak kasatmata ini bergantung pada kemampuan komunitas global untuk berkolaborasi dan berbagi intelijen secara efektif. Pentingnya dialog internasional tidak bisa diremehkan, mengingat bahwa ancaman ini tidak mengenal batas negara dan dapat meredam upaya yang paling canggih sekalipun jika dilakukan secara terisolasi. Kolaborasi antara badan-badan keamanan, pertukaran informasi lintas batas, dan kerangka kerja hukum

internasional baru diperlukan untuk meredam kekacauan dan menciptakan sistem yang tangguh terhadap tantangan masa depan.

Begitu pula, kita tidak bisa mengabaikan peran warga sipil dalam menghadapi ancaman ini (Hikam, 2017). Edukasi publik yang tepat mengenai sifat ancaman terorisme dan upaya peningkatan kesadaran adalah langkah kritis dalam membangun masyarakat yang resisten terhadap retorika ekstrem dan propaganda yang memecah belah.

Dalam era dunia baru, ketidakpastian sudah menjadi bagian dari kehidupan sehari-hari, sementara musuh tak kasatmata mengintip dari balik layar kenyataan kita. Untuk menghadapinya, diperlukan inovasi berpikir, reformasi kebijakan, dan kolaborasi tanpa batas. Sejarah telah mengajarkan bahwa ancaman tidak dapat sepenuhnya dihilangkan, tetapi dengan usaha kolektif yang berkelanjutan, mereka dapat diminimalisir dan dikendalikan. Dunia baru mungkin dipenuhi dengan ketidakpastian, tetapi ini juga memberikan peluang untuk memperkuat fondasi keamanan internasional yang lebih manusiawi dan adil.

### 1.1.1 Multipolaritas dan Runtuhnya Tatanan Dominan

Dalam dunia yang semakin kompleks dan terhubung, era multipolaritas telah menandai runtuhnya tatanan dominan yang sebelumnya digawangi oleh kekuatan-kekuatan besar pasca-Perang Dunia II. Tidak seperti dalam masa perang dingin ketika dunia terpecah menjadi dua blok kekuatan, kini kita menyaksikan pergeseran keseimbangan kekuasaan yang lebih tersebar dan dinamis (Buzan & Waever, 2003; Freedman, 2006; Keersmaeker, 2017). Kondisi ini menandai kebangkitan berbagai pusat kekuatan baru baik negara maupun non-negara yang memainkan peran penting dalam arsitektur keamanan internasional, menciptakan ketidakpastian baru yang menantang sistem global.

Ketidakpastian ini diperburuk oleh sejumlah faktor, termasuk kebangkitan ekonomi negara-negara berkembang, transformasi teknologi militer, pergeseran hubungan diplomatis, serta ancaman non-tradisional seperti terorisme dan serangan siber. Dalam konteks ini, multipolaritas tidak hanya menciptakan peluang tetapi juga ancaman

yang kompleks (Trends Research & Advisory, 2025), terutama dalam memformulasikan dan menerapkan kebijakan keamanan yang adaptif dan responsif.

Era multipolaritas memperlihatkan kebangkitan kekuatan ekonomi baru, seperti Tiongkok dan India, yang mengganggu keseimbangan dominasi Barat dalam ekonomi global (Trends Research & Advisory, 2025). Tiongkok, dengan pertumbuhan ekonomi yang mengesankan dan ambisi geopolitiknya, secara aktif meningkatkan pengaruh melalui inisiatif seperti *Belt and Road Initiative* (BRI). Proyek ambisius ini tidak hanya mengubah lanskap ekonomi di berbagai belahan dunia tetapi juga menantang kebijakan luar negeri tradisional negara-negara Barat dan membuka alur baru dalam arsitektur diplomasi internasional.

Kebangkitan kekuatan tersebut menimbulkan beberapa ketidakpastian, misalnya dalam hal perang dagang, kesenjangan ekonomi, dan dominasi teknologi. Contohnya dapat kita lihat dari persaingan ketat antara AS dan Tiongkok dalam teknologi 5G, di mana perlombaan untuk mendapatkan supremasi teknologi ini melibatkan peluncuran inovasi teknologi serta benturan kepentingan di berbagai forum perdagangan dunia (Harwit, 2023). Ketidakpastian ini menciptakan kekhawatiran tentang dominasi dan keamanan siber yang diperebutkan dalam tataran internasional.

Selain ekonomi, transformasi teknologi militer juga menjadi faktor penentu dalam menciptakan ketidakpastian. Pengembangan persenjataan canggih seperti drone, sistem pertahanan rudal, dan kecerdasan buatan (*Artificial Intelligence*/AI) telah mengubah nilai strategis kekuatan militer tradisional (Atkinson, 2024). Negara-negara bersaing dalam inovasi teknologi militer yang menghadirkan ancaman baru dan tak terduga sebuah medan perang futuristik yang rentan terhadap perubahan taktis mendadak.

Teknologi seperti AI sedang diimplementasikan dalam operasi militer yang menciptakan tantangan etika dan keamanan yang belum terpecahkan (Schwarz, 2024; Islam & Wasi, 2024). Serangan siber yang menargetkan infrastruktur kritis, identitas pribadi, dan sistem pemerintahan semakin sering terjadi, menciptakan mimpi buruk bagi

keamanan global. Contoh nyata sehari-hari terlihat pada insiden-insiden peretasan terhadap sistem pemerintah dan perusahaan besar yang melibatkan pencurian informasi dan sabotase ekonomi (Annur, 2022). Hal ini menambah dimensi baru dalam lingkup keamanan yang tak lagi terbatas pada batasan geografis.

Di tengah multipolaritas ini, hubungan diplomatik juga mengalami pergeseran signifikan. Aliansi tradisional dipertanyakan kembali, dan pendekatan multilateral sering kali tergantikan oleh tindakan unilateralisme dan nasionalisme ekstrem seperti yang dilakukan oleh Presiden Trump akhir-akhir ini. Contoh lain dapat dilihat dari keluarnya Inggris dari Uni Eropa atau Brexit, yang menciptakan ketidakpastian dalam persatuan ekonomi dan politik Eropa (Sugiono, 2020).

Tak hanya di Eropa, dampak pergolakan diplomatik ini terasa pula di Timur Tengah dan Asia, di mana variabel-variabel baru dalam politik regional sering kali memicu ketidakstabilan yang lebih luas. Proliferasi senjata di Korea Utara, ketegangan geografis politik di Laut Tiongkok Selatan, dan perseteruan panjang Palestina-Israel merupakan beberapa contoh fenomena yang menegaskan kompleksitas diplomasi modern, menantang arsitektur keamanan yang ada.

Salah satu aspek paling meresahkan dari ketidakpastian dalam arsitektur global saat ini adalah ancaman non-tradisional yang diwakili oleh aktor-aktor non-negara seperti kelompok teroris dan jaringan kriminal internasional (Breslin, 2002; Hoffman, 2006). Banyak dari ancaman ini lebih sulit ditangani karena sifat mereka yang tak terduga dan tersebar, serta kemampuan mereka untuk beradaptasi dengan cepat terhadap langkah-langkah penegakan hukum yang ketat.

Serangan teroris yang terorganisir, terkoordinasi dan beroperasi dengan canggih yang dilakukan oleh kelompok-kelompok seperti ISIS dan Al-Qaeda telah menunjukkan ketahanan dan kemampuan mereka untuk memanipulasi kerentanan struktur sosial dan teknologi untuk mencapai tujuan mereka. Misalnya, serangan teroris yang menargetkan ruang publik, seperti pemboman di Paris pada 2015, tidak hanya bertujuan untuk menciptakan rasa takut tetapi juga mempengaruhi kebijakan politik dan sosial (Christiastuti 2015).

Meski menghadapi ketidakpastian yang besar, era multipolaritas juga memberikan peluang untuk pendekatan multilateral dan integrasi internasional yang lebih erat. Perserikatan Bangsa-Bangsa (PBB) dan organisasi internasional lainnya berusaha mengadopsi peran sentral dalam mediasi dan penegakan hukum internasional. Tujuannya adalah untuk memfasilitasi kolaborasi negara-negara dalam mengatasi tantangan bersama.

Dialog-dialog seperti negosiasi iklim global dan kerja sama penanggulangan bencana serta terorisme, menjadi penting dalam mengelola ancaman yang bersifat global dan lintas batas negara. Meski demikian, efektivitas lembaga-lembaga ini sering kali terancam oleh kepentingan nasional yang berbeda dan tuntutan politik yang kontradiktif (Parikesit & Wairocana, 2017). Sehingga mengisyaratkan perlunya komitmen yang lebih kuat terhadap prinsip-prinsip hukum internasional dan kolaborasi jangka panjang dalam mengejar keamanan kolektif.

Dalam menghadapi ketidakpastian ini, strategi intelijen memiliki peran sentral dalam melindungi kepentingan nasional dan internasional. Di masa kini, operasi intelijen tidak lagi terbatas pada pemantauan militer tetapi mencakup segala aspek informasi dari ekonomi, teknologi hingga sosial (Mulya, 2025). Pengumpulan, pemilahan dan analisis data menjadi esensial dalam mengambil keputusan yang tepat dan cepat dalam menghadapi krisis.

Misalnya, teknologi pengenalan wajah dan analisis *big data* digunakan untuk memantau kegiatan teroris dan mengidentifikasi pola-pola perilaku yang dapat menandakan ancaman yang akan datang (Nurrochman, 2024). Namun, strategi ini menimbulkan kekhawatiran mengenai privasi, etika dan hak asasi manusia, sehingga menuntut kebijakan dan pengawasan yang hati-hati untuk menjaga keseimbangan antara keamanan dan kebebasan individu.

Untuk mengelola ketidakpastian dan menjaga stabilitas dalam arsitektur keamanan internasional, penting bagi negara-negara untuk mengembangkan kebijakan yang adaptif dan inklusif. Kondisi ini membutuhkan kesediaan untuk berkolaborasi melintasi batas-batas ideologis dan geografi, serta investasi dalam membangun kapasitas

internal dan regional untuk menanggapi perubahan mendadak dan ancaman yang muncul.

Pembangunan ketahanan sosial dan ekonomi juga menjadi bagian penting dari strategi ini karena kestabilan internal merupakan fondasi yang kuat untuk berpartisipasi dalam keamanan global. Kontribusi dalam memperkuat lembaga-lembaga negara, pendidikan, dan inklusi perempuan dan ekonomi harus dilihat sebagai komponen vital dalam strategi keamanan yang komprehensif.

Sebagai hasil dari multipolaritas dan kompleksitas global, era modern ini menawarkan dinamika arsitektur keamanan internasional yang penuh ketidakpastian namun juga penuh dengan peluang untuk inovasi dalam diplomasi dan keamanan. Dengan memanfaatkan teknologi canggih, memperkuat struktur sosio-ekonomi, dan meningkatkan kerjasama internasional, kita dapat membangun dunia yang lebih aman dan tangguh di mana ancaman nyata dan tidak nyata dapat dihadapi secara efektif. Upaya-upaya kolektif untuk menghadapi tantangan global adalah kunci untuk memastikan stabilitas dan kemakmuran generasi mendatang di tengah arus perubahan yang tak terelakkan.

### 1.1.2 Perang Tak Dinyatakan, Konflik Tetap Terjadi

Dalam bab ini, kita memulai dengan menggambarkan perubahan dinamis yang melanda arsitektur global sejak akhir Perang Dingin. Tidak ada satu pun tatanan yang bisa dianggap sepenuhnya stabil dalam dunia kita saat ini, dan ini terutama berkaitan dengan kebangkitan musuh-musuh tak kasatmata yang mengancam keamanan internasional. Arsitektur global yang dahulu dianggap kuat dan terstruktur kini menghadapi ketidakpastian yang mengintensif. Berbagai aktor non-negara, seperti jaringan teroris dan sindikat kejahatan transnasional, telah muncul sebagai ancaman nyata. Ini adalah ancaman yang tak mudah dideteksi dengan kaidah tradisional, memerlukan respons kreatif dan fleksibel yang juga berdampak pada dinamika internasional.

Sebelumnya, ancaman terhadap keamanan suatu negara biasanya datang dari kekuatan militer negara lain, jelas dan terlihat. Namun, saat

ini ancaman lebih sering muncul secara diam-diam, bersembunyi di balik bayang-bayang digital dan jejaring sosial. Kelompok Al-Qaeda, yang bertanggung jawab atas serangan 11 September 2001 di Amerika Serikat, adalah contoh yang mengguncang dunia mengenai betapa berbahayanya organisasi yang beroperasi di luar struktur negara. Kebanyakan dari kita masih jelas mengingat hari itu, bagaimana rasa aman yang selama ini melekat pada sebuah negara adidaya seketika runtuh di depan mata kita.

Transisi menuju ketidakpastian ini tidak sedikit dimotori oleh globalisasi dan perkembangan teknologi yang pesat. Keterhubungan dunia yang semakin erat menciptakan paradoks: di satu sisi, ia menawarkan peluang untuk pertumbuhan ekonomi dan kerjasama internasional, namun di sisi lain, ia membuka celah bagi aktivitas ilegal dan berbahaya untuk berkembang lebih jauh (Stiglitz, 2002; Damanhuri, 2008). Internet telah menjadi medan pertempuran baru, dengan serangan siber yang dapat menjatuhkan infrastruktur penting suatu negara sama efektifnya, jika tidak lebih, dari sebuah invasi militer.

Sebagai contoh, kita bisa melihat serangan siber pada sistem distribusi listrik di Ukraina beberapa tahun yang lalu (Sarimin & Damayanti, 2024). Ketika pemadaman listrik terjadi dan meninggalkan ribuan rumah dalam kegelapan, hanya dalam beberapa jam, efek psikologis dan sosialnya sangat terasa. Serangan tersebut diduga berasal dari kelompok aktor non-negara yang didukung oleh negara besar, dan ini menunjukkan bagaimana batas antara perang konvensional dan aktivitas kriminal semakin kabur.

Di tengah situasi ini, intervensi militer tradisional tidak lagi menimbulkan efek penangkalan yang sama. Negara-negara kini harus memikirkan ulang pendekatan keamanan mereka, dengan mempertimbangkan bagaimana intelijen dapat berperan dalam mendeteksi dan menetralisir ancaman sebelum berkembang menjadi krisis. Kerjasama intelijen antara sekutu menjadi lebih diandalkan daripada sebelumnya. Pembagian informasi secara proaktif memegang peranan penting dalam usaha menghadapi ancaman yang sulit terdeteksi ini (Lowenthal, 2017; Warner, 2014).

Namun, pembagian informasi ini tidak bebas dari masalah. Ketidakpercayaan yang pernah terjadi di masa lalu seringkali mengganggu komunikasi efektif antarnegara atau bahkan antar-agen dalam satu negara. Banyak pihak masih enggan untuk sepenuhnya membuka jaringan mereka, mengkhawatirkan kebocoran data sensitif atau penyalahgunaan informasi. Kita melihat contoh ini pada kebocoran informasi pengawasan oleh Edward Snowden yang memicu kontroversi global mengenai privasi dan penyadapan oleh badan intelijen negara.

Untuk menjawab tantangan dalam sistem global yang semakin majemuk ini, negara-negara perlu memperkuat kerangka kerja multilateral baru yang lebih inklusif dan adaptif. Tetapi, membangun konsensus dalam dunia yang beraneka ragam adalah tugas berat. Setiap negara memiliki kepentingan dan pendekatan yang berbeda dalam mengatasi ancaman terorisme dan kejahatan siber (Nye & Welch, 2017). Diplomasi memainkan peran krusial dalam menyelaraskan pandangan yang berbeda ini, mencoba mengarahkan dialog ke arah tindakan kolektif yang lebih efektif. Contohnya, pakta keamanan regional seperti NATO di Eropa telah berevolusi untuk menghadapi ancaman yang sebelumnya tidak mereka perhitungkan (Webber, Sperling, Smith, 2012).

Ketidakpastian arsitektur global ini juga muncul dari kebangkitan ekonomi pasar-pasar baru yang menguatkan aktor non-negara. Negara-negara berkembang yang mengalami pertumbuhan ekonomi yang cepat, sering kali mendapati diri mereka menjadi lahan subur bagi rekrutmen dan pendanaan kelompok teror (Krueger, 2007). Misalnya, penggunaan narasi ekstremis dalam menarik orang-orang yang kesulitan mencari kerja di daerah-daerah serta mengalami kesenjangan ekonomi dan sosial menunjukkan betapa pentingnya pekerjaan dalam bidang ekonomi untuk mencegah radikalisasi.

Selain itu, pendidikan menjadi sekutu tak ternilai dalam perang melawan terorisme yang berakar pada ideologi kebencian. Dengan mengedepankan pendidikan yang inklusif dan mempromosikan toleransi, masyarakat dapat berperan aktif, termasuk perempuan dan generasi muda, dalam mencegah penyebaran radikalisasi (Davies, 2009; Sas, et.al., 2020). Reformasi dalam sistem pendidikan di berbagai negara

telah menunjukkan dampak yang signifikan. Pemerintah negara-negara seperti Arab Saudi telah melaksanakan pembenahan kurikulum untuk menghilangkan ajaran yang dapat mendorong ekstremisme (Burbridge, Patton & al-Waheidi, 2022), dan ditambah program-program keterlibatan masyarakat yang melibatkan para pemimpin agama lokal dalam menyebarkan pesan damai (Malahayati, 2022).

Pembahasan mengenai ketidakpastian dalam arsitektur global ini adalah refleksi dari dunia yang berada di tengah transformasi besar. Seiring dengan upaya negara-negara untuk lebih mewaspadai ancaman dan memupuk kerja sama lintas batas yang lebih baik, penerimaan dan adaptasi terhadap cara-cara baru dalam berpikir tentang keamanan menjadi kunci. Bersahabat dengan ketidakpastian berarti mengakui bahwa dunia tidak lagi bisa didikte oleh kekuatan militer semata. Dunia baru ini adalah dunia di mana konektivitas dan informasi menjadi alat sekaligus senjata, sehingga mendorong semua orang, negara dan individu berperan dalam menjaga perdamaian dan keamanan.

Kita harus belajar untuk bekerja dalam ketidakpastian ini, menganggapnya bukan sebagai ancaman semata, tetapi sebagai peluang untuk menciptakan sistem yang lebih tangguh dan inklusif. Sebab, di balik setiap ancaman terletak kesempatan untuk memperkuat ikatan global dalam menghadapi segala bentuk kekerasan dan kebencian. Sementara arsitektur global yang mewujud di hadapan kita tampak rapuh, pada saat yang sama, ia juga menyiratkan potensi untuk menciptakan dunia yang lebih adil dan aman, jika komunitas internasional memilih untuk bekerja bersama menuju tujuan tersebut.

## 1.2 Ancaman Non-Negara dalam Sistem Internasional

Dalam era globalisasi yang terus berkembang, sistem internasional menghadapi tantangan yang semakin kompleks dan dinamis. Salah satu fenomena yang mencolok dalam lanskap ini adalah munculnya ancaman non-negara, yang sering kali beraksi dalam bayang-bayang, menjadi musuh tak kasatmata yang sulit dideteksi dan diantisipasi. Ancaman-ancaman ini tidak hanya memengaruhi keamanan negara,

tetapi juga mengguncang arsitektur keamanan internasional secara keseluruhan, mendorong para pembuat kebijakan dan komunitas intelijen untuk menyusun strategi yang lebih adaptif dan inovatif.

Ancaman non-negara bisa didefinisikan sebagai entitas atau aktor yang tidak berafiliasi dengan negara tertentu, tetapi memiliki kapasitas untuk memengaruhi keamanan dan stabilitas internasional (Breslin, 2002; Arquilla & Ronfeldt, 2001). Salah satu aspek utama dari ancaman ini adalah sifatnya yang tidak terikat oleh batasan geografis atau hukum internasional, sehingga memberikan mereka kapasitas untuk beroperasi secara bebas di ruang virtual dan fisik. Sebagai contoh, kelompok teroris transnasional seperti Al-Qaeda dan ISIS memanfaatkan teknologi komunikasi modern untuk menyebarkan ideologi ekstremis, merekrut anggota di berbagai belahan dunia, mengumpulkan donasi, serta merencanakan dan melaksanakan serangan tanpa perlu mematuhi norma-norma tradisional dalam perang (Winter, 2015; Klausen, 2015).

Dalam konteks dunia baru yang semakin terhubung secara digital, ancaman siber juga telah menjadi salah satu bentuk ancaman non-negara yang paling signifikan. Ini tidak hanya melibatkan serangan terhadap infrastruktur kritis, tetapi juga mencakup pencurian data pribadi, spionase korporat, dan disinformasi yang dapat menggoyahkan demokrasi (Solove, 2007). Seiring dengan perkembangan teknologi yang pesat, pelaku-pelaku ini cenderung lebih sulit dilacak dan diidentifikasi. Serangan siber sering kali dilakukan dari jarak jauh, menggunakan jaringan botnet yang menyebar di berbagai negara, membuat pelaku dapat menyamarkan jejak mereka dan memanfaatkan kerentanan sistem untuk keuntungan mereka sendiri.

Pembajakan modern juga kembali menjadi ancaman yang mengkhawatirkan. Memanfaatkan keberanian dan ketangkasan, kelompok-kelompok ini menyerang kapal-kapal dagang internasional, terutama di kawasan rawan seperti Teluk Aden dan perairan sekitar Somalia (Chalk, 2010; Middleton, 2012; Bueger, 2015). Meskipun berakar pada isu ekonomi dan politik lokal, dampak dari aktivitas ini meluas hingga mengganggu jalur perdagangan internasional dan menimbulkan kerugian ekonomi yang signifikan. Banyak negara kini harus

mengerahkan angkatan laut mereka untuk melindungi jalur pelayaran, menambahkan lapisan baru pada tantangan keamanan maritim global.

Ancaman non-negara lainnya yang menyita perhatian internasional adalah perdagangan manusia dan narkotika. Kedua kegiatan ilegal ini tidak hanya mendatangkan profit bagi organisasi kriminal transnasional, tetapi juga melemahkan stabilitas sosial dan politik di banyak negara (Shelley, 2010; Andreas, 2009a). Pergerakan manusia secara paksa menciptakan krisis kemanusiaan yang berkelanjutan, sementara penyelundupan narkotika yang melintasi batas negara merusak tatanan hukum dan menciptakan masalah kesehatan masyarakat yang luas.

Bagaimanapun, salah satu karakteristik paling mencolok dari ancaman non-negara adalah sifatnya yang cair dan adaptif. Tidak seperti ancaman negara yang berdasarkan pada kekuatan militer konvensional dan diplomasi yang terstruktur, ancaman non-negara cenderung bersifat asimetris. Mereka dapat menyesuaikan diri dengan cepat terhadap perubahan lingkungan dan menggunakan strategi gerilya untuk menghindari konfrontasi langsung dengan pasukan bersenjata tradisional. Fleksibilitas inilah yang membuat mereka lebih sulit untuk dihadapi dengan cara-cara konvensional.

Di tengah tantangan ini, peran intelijen menjadi sangat vital. Berbeda dengan ancaman dari negara lain yang sering kali dapat diprediksi melalui analisis politik dan militer konvensional, ancaman non-negara membutuhkan metode pemantauan dan analisis yang lebih inovatif. Pengumpulan data intelijen dari berbagai sumber, baik sinyal elektronik maupun sumber manusia, menjadi sangat penting untuk memahami jaringan dan motif di balik ancaman ini. Teknologi pengolahan dan analisis *big data* kini menjadi alat yang krusial dalam memilah informasi yang relevan dari tsunami data yang tersedia.

Selain itu, ancaman non-negara memerlukan bentuk kerjasama internasional yang lebih erat dan efektif. Keberhasilan dalam menangani masalah ini tidak dapat dicapai secara individu oleh satu negara saja. Membangun koalisi internasional, berbagi intelijen lintas negara, dan menyelaraskan kebijakan hukum menjadi kunci dalam menghadapi ancaman yang tidak mengenal batas ini. Forum-forum seperti Interpol,

PBB, dan kerja sama regional menjadi platform bagi negara-negara untuk saling bertukar informasi dan strategi.

Namun, upaya untuk menghadapi ancaman non-negara tidak boleh mengorbankan nilai-nilai demokrasi dan hak asasi manusia. Dalam banyak kasus, kebijakan yang terlalu represif justru dapat memicu reaksi balik yang memperburuk masalah. Pendekatan yang lebih manusiawi, dengan mengedepankan dialog, pencegahan, dan rehabilitasi, harus menjadi bagian integral dari strategi yang diterapkan. Pendidikan dan pengetahuan mengenai bahaya ekstremisme dan kriminalitas adalah langkah preventif yang krusial, terutama dalam menciptakan generasi masa depan yang tangguh dan berdaya.

Perubahan struktur internasional, baik dalam aspek politik maupun sosial-ekonomi, mengisyaratkan bahwa ancaman non-negara akan terus menjadi bagian dari lanskap keamanan global (Breslin, 2002). Tantangan yang dihadapi mungkin akan semakin kompleks seiring dengan perkembangan teknologi dan dinamisnya relasi antarnegara. Namun, dengan pemahaman yang lebih baik mengenai karakteristik dan modus operandi ancaman ini, serta komitmen untuk meningkatkan kerja sama internasional, dunia dapat lebih siap dan tanggap dalam menghadapi musuh-musuh tak kasatmata yang terus mengintai dari balik layar.

Menghadapi ancaman non-negara memerlukan perubahan paradigma dalam memahami konsep keamanan dan pertahanan internasional. Kita harus bersedia untuk melampaui batas-batas tradisional, mengadopsi pendekatan yang lebih terbuka dan kolaboratif, dan mengintegrasikan berbagai disiplin ilmu untuk merancang strategi yang komprehensif dan berkelanjutan.

Dunia baru mengundang kita untuk membuka mata terhadap ancaman yang tidak lagi terikat pada pengertian lama tentang perang dan konflik, tetapi melibatkan dimensi baru di mana ideologi, informasi, dan teknologi menjadi senjata yang menentukan medan pertempuran. Dengan musuh yang tak kasatmata ini, setiap individu dan negara dituntut untuk waspada dan adaptif dalam menavigasi tantangan kompleks abad ke-21.

### 1.2.1 Aktor Tanpa Bendera: Terorisme dan Organisasi Gelap

Pada era globalisasi yang semakin terhubung ini, kita menyaksikan perubahan dramatis dalam cara ancaman dialami dan diatasi oleh negara-bangsa. Ancaman yang datang bukan lagi didominasi oleh negara lain, melainkan sering kali berasal dari entitas non-negara, seperti terorisme, organisasi kriminal transnasional, dan kelompok pemberontak. Ancaman semacam ini sulit diprediksi dan ditangani karena mereka beroperasi lintas batas dan berbentuk jaringan yang terdesentralisasi, serta memanfaatkan perkembangan teknologi untuk memperkuat pengaruh mereka. Maka, era hari ini sering disebut sebagai zaman di mana terorisme dan organisasi gelap adalah musuh utama yang tak kasatmata.

Sejak serangan 11 September 2001, terorisme telah menjadi fokus utama kebijakan keamanan internasional. Kelompok-kelompok seperti Al-Qaeda dan belakangan ISIS telah menunjukkan kemampuan untuk menebar ketakutan bukan hanya melalui tindakan kekerasan fisik tetapi juga melalui perang psikologis (Arquilla & Ronfeldt, 2001; Hoffman, 2006). Dalam konteks global, mereka mampu merekrut individu dari berbagai negara, memanfaatkan media sosial sebagai alat propaganda dan pengumpulan dana, serta menyusup ke komunitas-komunitas lokal untuk menyebarkan ideologi mereka (Awan, 2011). Strategi ini tidak hanya bertujuan merusak keamanan fisik, tetapi juga menyerang keberagaman budaya dan ketentraman masyarakat.

Di banyak negara, ancaman ini diperparah oleh kehadiran kelompok-kelompok ekstremis yang mencari legitimasi politik melalui tindakan teror. Di Indonesia, misalnya, kita mencatat jaringan teroris lokal atau individu yang terkait dengan ISIS berupaya mengganggu stabilitas dengan melakukan serangan bom bunuh diri, seperti yang terjadi di Surabaya pada Mei 2018 atau penusukan Menkopolhukam Wiranto pada Oktober 2019. Tindakan semacam ini memaksa aparat keamanan untuk memperkuat kemampuan intelijen, mempererat kerjasama internasional, serta melibatkan masyarakat dalam mendeteksi ancaman lebih dini.

Namun, organisasi gelap tak terbatas pada terorisme saja. Kita juga menghadapi ancaman dari jaringan perdagangan narkoba dan penyelundupan manusia yang beroperasi di bawah radar. Organisasi kriminal ini sering memiliki hubungan simbiotik dengan kelompok teror, memanfaatkan kekacauan untuk menjalankan operasi ilegal dan mencuci uang mereka. Mereka menyedot sumber daya ekonomi negara, memperlemah institusi penegak hukum, dan sering kali melibatkan diri dalam kegiatan korupsi yang merusak tatanan sosial (Andreas, 2009a; Shelley, 2010).

Di wilayah Amerika Latin, kartel narkoba seperti Sinaloa menunjukkan bagaimana sekelompok organisasi gelap dapat menciptakan negara dalam negara (Paoli, Peters, Reuter, 2024). Mereka memiliki milisi bersenjata, jaringan intelijen, dan kebijakan luar negeri sendiri dengan sering mempengaruhi keputusan politik lokal. Tuduhan inilah yang digunakan Trump untuk menangkap Presiden Venezuela, Nicolas Maduro pada awal Januari 2026. Maduro dianggap mendukung jaringan narkotika transnasional. Di Eropa dan AS, perdagangan narkoba yang dilakukan oleh kelompok-kelompok tersebut menjadi pendorong utama kejahatan dan kekerasan di kota-kota besar, memperumit upaya polisi untuk menjaga keamanan publik.

Dengan kemajuan teknologi, aktor-aktor non-negara ini menemukan cara baru untuk menghindari deteksi dan pemberantasan. *Dark web* menjadi pasar yang subur untuk perdagangan senjata ilegal, narkoba, dan bahkan layanan peretasan yang dapat digunakan untuk melancarkan serangan siber terhadap infrastruktur negara. Di tahun 2017, serangan ransomware WannaCry mengunci komputer-komputer di lembaga-lembaga kesehatan dan bisnis di seluruh dunia, menunjukkan betapa rentannya infrastruktur kita terhadap serangan yang dilancarkan oleh kelompok-kelompok dengan motivasi anasir politik maupun ekonomi (Yusuf, 2017).

Peran intelijen pun menjadi semakin krusial dalam menghadapi ancaman non-negara ini. Informasi menjadi kunci dalam merespon cepat ancaman yang bergerak dinamis. Namun, pengumpulan data intelijen membawa tantangan etis dan operasional tersendiri. Di satu

sisi, pemerintah perlu menjaga keamanan rakyatnya, tetapi di sisi lain, masyarakat semakin kritis terhadap upaya pengintaian yang melanggar hak privasi (Miller, Regan & Walsh, 2022). Skandal informasi publik seperti yang diungkapkan oleh Edward Snowden pada 2013, misalnya, melahirkan skeptisisme global terhadap sejauh mana pemerintah dapat dipercaya untuk mengelola pengawasan warga negaranya.

Itu sebabnya, kerjasama internasional menjadi bagian penting dari solusi. Ancaman global tidak bisa dihadapi sendirian. Negara-negara perlu bekerja sama, berbagi informasi intelijen dan mengembangkan strategi penanganan yang komprehensif. Contoh sukses dari kerjasama ini dapat dilihat dari peran Interpol dan badan-badan serupa dalam mengkoordinasikan respon terhadap pedagang narkoba dan teroris lintas negara. Namun, kerjasama ini pun tidak bebas dari komplikasi. Ada ketegangan dalam hal kedaulatan negara, berbagi informasi rahasia, dan perbedaan dalam pendekatan kebijakan antiterorisme dan keamanan nasional.

Di tengah tantangan bombastis ini, solusi yang benar juga melibatkan upaya mencegah radikalisasi di akar rumput. Elemen-elemen kunci seperti pendidikan, kesempatan ekonomi, dan dialog komunitas sering kali diabaikan tetapi sebenarnya kritis dalam menyebarluaskan konsep toleransi dan menolak ekstremisme. Ada banyak program yang bertujuan untuk mengatasi masalah-masalah ini, seperti yang dilakukan oleh organisasi non-pemerintah yang fokus pada deradikalisasi mantan ekstremis, yang memberikan wawasan dan pendidikan untuk memungkinkan integrasi mereka kembali ke masyarakat (Sas, et.al., 2020).

Dunia baru yang kita hadapi saat ini adalah panggung bagi kenyataan kompleks di mana musuh tak kasatmata beroperasi. Mereka bukan hanya ujian bagi keamanan internasional, tetapi juga bagi sejauh mana kita bisa menjunjung nilai-nilai kebebasan, keadilan, dan hak asasi manusia. Melihat ancaman ini sebagai kesempatan untuk bersatu dan memperkuat jaringan internasional kita, dengan tetap memelihara hak-hak dasar, adalah tantangan terbesar yang harus kita hadapi. Dunia terus berubah, dan dalam perubahan itu, kita harus menjadi lebih kuat serta

lebih bijaksana dalam menghadapi ancaman non-negara pada sistem internasional.

### 1.2.2 Dilema Negara: Batas Wilayah vs Ancaman Lintas Negara

Dalam lanskap geopolitik modern, batas wilayah negara telah lama menjadi fitur yang mendominasi penentuan kedaulatan dan hak yurisdiksi. Namun, di era globalisasi yang kita jalani saat ini, batas-batas negara semakin terlihat kabur ketika berhadapan dengan ancaman lintas negara yang kian meningkat. Ancaman ini tidak hanya menantang otoritas negara dalam melindungi warganya, tetapi juga mengguncang fondasi sistem internasional yang didasarkan pada kedaulatan teritorial.

Ancaman non-negara mencakup berbagai bentuk kekerasan dan ketidakstabilan yang dipicu atau diakibatkan oleh aktor-aktor yang tidak terikat pada entitas negara tertentu. Bentuk ancaman ini bisa berupa terorisme, kelompok pemberontak, kartel narkoba, organisasi kriminal transnasional, atau bahkan serangan siber yang dilancarkan individu atau kelompok independen. Ancaman-ancaman ini umumnya terorganisasi, memiliki jaringan global, dan sering kali lebih lincah dibandingkan dengan struktur negara yang kaku (Breslin, 2002).

Satu contoh nyata adalah terorisme internasional yang telah menciptakan ancaman keamanan global tanpa memandang batas wilayah. Organisasi seperti Al-Qaeda dan ISIS telah memperlihatkan bagaimana kelompok-kelompok ini dapat memanfaatkan teknologi modern seperti internet untuk merekrut, menginspirasi, menggalang dana dan mengoordinasikan serangan dari jarak jauh (Hoffman, 2006). Ini menimbulkan tantangan berat bagi negara-negara yang harus beradaptasi dengan strategi keamanan yang tidak lagi dapat berpaku pada penegakan hukum konvensional berbasis wilayah.

Selain terorisme, ancaman siber telah muncul sebagai salah satu bentuk ancaman non-negara yang paling signifikan. Dengan teknologi informasi yang menyentuh hampir setiap aspek kehidupan modern, serangan siber memiliki potensi untuk mengacaukan ekonomi, infrastruktur penting, dan privasi individu tanpa memandang batas

negara (Singer & Friedman, 2014). Misalnya, peretasan besar-besaran terhadap perusahaan multinasional atau lembaga pemerintahan dapat dilakukan dari jarak ribuan mil jauhnya, sering kali oleh aktor yang tak terdeteksi atau berasal dari berbagai negara.

Bahkan, gerakan-gerakan separatis atau pemberontak sering kali mendapatkan dukungan dari jaringan internasional yang melibatkan berbagai aktor non-negara. Misalnya, konflik di Suriah telah melibatkan berbagai milisi yang mendapat dukungan dari organisasi internasional atau bahkan dari negara lain yang memiliki agenda tertentu (Phillips, 2016). Dukungan ini bisa berupa perlengkapan senjata, pelatihan militer, hingga dukungan finansial yang disalurkan melalui saluran yang tidak mudah dideteksi.

Kartel narkoba dan organisasi kriminal transnasional lainnya menambah kompleksitas ancaman non-negara ini. Mereka beroperasi melewati batas-batas negara, memanfaatkan celah-celah dalam sistem hukum dan perbatasan yang kurang terjaga. Perdagangan narkoba, perdagangan manusia, dan penyelundupan barang ilegal adalah bagian dari operasi mereka yang sering kali melibatkan kolusi dengan oknum pemerintah atau aparat penegak hukum, baik secara langsung maupun tidak langsung (Andreas, 2009 a; Shelley, 2010).

Mobilitas tinggi dan globalisasi ekonomi memberikan keuntungan bagi jaringan kejahatan ini untuk mengaburkan jejak mereka, menyembunyikan keuntungan mereka dalam sistem finansial dunia yang terintegrasi, dan menghindari penegakan hukum dengan berpindah-pindah yurisdiksi. Operasi-operasi ini menimbulkan tantangan besar bagi negara yang berjuang untuk mempertahankan hukum dan ketertiban dalam batas teritorial mereka.

Pada tatanan yang lebih sistemik, globalisasi telah membuka jalur baru untuk penyebaran ideologi ekstrem. Internet dan media sosial memainkan peran kunci dalam hal ini, memberikan platform bagi ide-ide radikal untuk menyebar lintas batas tanpa hambatan (Awan, 2011; Seib & Janbek, 2011). Hal ini menantang institusi negara yang berusaha mengontrol narasi atau diskursus tertentu di dalam wilayah mereka. Proliferasi ideologi ekstrem dan kemampuan rekrutmen melalui dunia

maya ini memperlihatkan bagaimana ancaman non-negara menimbulkan risiko tidak hanya secara fisik tetapi juga ideologis.

Respons negara terhadap ancaman-ancaman ini sering kali harus bersifat internasional. Inisiatif multilateral menjadi lebih penting seiring dengan meningkatnya ancaman lintas batas. Kolaborasi antar negara dalam bentuk berbagi intelijen, patroli perbatasan yang terkoordinasi, dan kerangka hukum internasional untuk penyelidikan kejahatan lintas negara menjadi elemen kunci dalam merespons ancaman non-negara (Lowenthal, 2017; Andreas, 2009 b).

Namun, ini tidak menghapus kebutuhan untuk melindungi kedaulatan negara. Setiap negara tetap bertanggung jawab utama atas keamanan dan kesejahteraan warga negaranya. Mereka harus memperkuat kemampuan mereka dalam mengelola ancaman non-negara ini melalui kebijakan domestik yang dirancang untuk mencegah radikalisasi, meningkatkan keamanan siber, dan memperketat penegakan hukum terhadap aktivitas kriminal internasional.

Ketegangan antara penegakan kedaulatan negara dan ancaman lintas negara ini menghadirkan dilema bagi pembuat kebijakan. Misalnya, perlindungan kebebasan sipil harus diseimbangkan dengan kebutuhan untuk keamanan nasional (Cole, 2005). Penyusunan kebijakan yang penyintas dan adil menjadi kebutuhan mendesak untuk menangani ancaman non-negara tanpa merusak nilai-nilai demokratis dan kemanusiaan (Hennebel & Tigroudja, 2011).

Di sisi lain, masyarakat internasional dituntut untuk memikirkan kembali konsep keamanan yang melampaui batas geografi tradisional, merefleksikan bahwa dinamika kekuatan global telah berubah. Dalam dunia yang semakin terhubung ini, suatu pelanggaran keamanan di satu bagian dunia berpotensi untuk menimbulkan efek riak yang mempengaruhi bagian lain. Edward Norton Lorenz pada tahun 1961 memperkenalkan istilah *"butterfly effect"* untuk menggambarkan kondisi keterhubungan sebab-akibat tersebut. Dengan demikian, pemahaman mengenai jaringan dan hubungan antara berbagai aktor baik itu negara, organisasi internasional, atau entitas non-negara menjadi penting dalam mengelola dan mencegah ancaman di era modern.

Secara khusus, kerjasama regional dapat menjadi solusi efektif dalam memerangi ancaman transnasional. Inisiatif seperti pertukaran informasi dan pelatihan bersama dapat meningkatkan kapabilitas negara-negara dalam menghadapi ancaman yang tidak hanya melintasi, tetapi juga tidak mengenal batas negara (Breslin, 2002). ASEAN misalnya, dianggap telah membantu negara-negara anggotanya untuk mengatasi ancaman-ancaman dari aktor non negara yang bersifat transnasional, melalui Komunitas Keamanan ASEAN (Acharya, 2014).

Contoh lainnya adalah koalisi global yang dibentuk untuk melawan ISIS. Negara-negara dari berbagai belahan dunia bekerja sama dalam operasi militer, berbagi intelijen, dan upaya kontra propaganda, menunjukkan bagaimana manajemen ancaman modern membutuhkan kerja sama lintas batas yang intensif dan terintegrasi (Rosand & Khan, 2021). Koalisi Global melawan ISIS ini merupakan kerjasama internasional yang bersifat komprehensif dalam menghadapi ancaman non-negara yang kompleks. Namun demikian, tantangan bisa terus berkembang, sehingga membutuhkan adaptasi berkelanjutan.

Dengan melihat contoh nyata dari ancaman dan respons internasional terhadap fenomena ini, jelas bahwa batas wilayah tradisional mengalami transformasi di tengah meningkatnya dinamika ancaman non-negara. Sistem keamanan internasional harus mampu berinovasi dan beradaptasi dengan realitas baru di mana ancaman dapat datang dari mana saja dan kapan saja, sering kali oleh aktor yang tidak terkait dengan negara. Seluruh masyarakat, mulai dari pemerintah hingga individu, harus meningkatkan kewaspadaan dan berpartisipasi aktif dalam pertahanan global melawan ancaman-ancaman modern yang tanpa batas.

Menghadapi semua ini, media juga memiliki peran penting dalam membentuk opini publik dan menyadarkan masyarakat tentang karakteristik ancaman baru ini. Meningkatkan literasi keamanan dan kesadaran akan risiko yang dihadirkan oleh ancaman non-negara dapat mendorong dukungan publik untuk kebijakan keamanan yang lebih efektif dan inklusif.

## 1.3 Intelijen sebagai Alat Kekuasaan Global

Pada tahun-tahun sebelum kejatuhan Tembok Berlin dan berakhirnya Perang Dingin, dunia terbelah dalam dua blok besar yang saling bertentangan: Barat yang dipimpin oleh Amerika Serikat dan Timur yang dikomandoi Uni Soviet. Kala itu, intelijen lebih sering berkutat pada upaya-upaya konvensional terkait perebutan informasi, penggalian rahasia militer, dan upaya-upaya kontra-intelijen lainnya. Namun, jatuhnya Uni Soviet mengubah lanskap geopolitik secara drastic (Buzan & Waever, 2003). Dunia yang tadinya bipolar kini menjadi multipolar, dan kekuatan intelijen menemukan diri mereka berada dalam sebuah paradigma baru di mana ancaman-ancaman tak kasatmata menjadi pusat perhatian (Appelbaum & Hadley, 2000).

Dalam dunia baru ini, ancaman tidak lagi datang dari arah yang telah dikenal sebelumnya. Terorisme, kejahatan transnasional dan konflik berskala kecil yang kerap dilandasi oleh ideologi ekstremis, telah menggantikan wajah musuh tradisional. Ketidakpastian ini menuntut pemikiran baru dalam menyusun strategi pertahanan dan keamanan suatu negara. Intelijen, yang dahulu lebih berfokus pada kemampuan militer besar dan perimbangan kekuatan, kini perlu mengarahkan pandangannya kepada jaringan teror dan kelompok-kelompok subnasional yang memiliki niat untuk mengacaukan kestabilan negara-negara berdaulat (Whitaker, 1992).

Pada era ini, intelijen berfungsi tidak hanya sebagai mata dan telinga negara, tetapi juga sebagai pedang di dalam bayangan. Setiap informasi yang dikumpulkan bisa berarti hidup atau mati jika salah diinterpretasikan (Hewitt, 2010). Dengan musuh yang berbentuk kelompok transnasional atau organisasi teroris yang tidak memiliki wajah atau alamat tetap, penilaian ancaman menjadi lebih rumit. Kini, intelijen harus bergerak cepat untuk melacak komunikasi digital, memantau transaksi keuangan ilegal, dan mengendus jejak kelompok yang beroperasi secara global namun tersembunyi di dunia maya.

Intelijen modern berkembang seiring pesatnya kemajuan teknologi (Gioe, Goodman & Stevens, 2020). Jika dahulu informasi disimpan dalam lemari arsip atau pita magnetik, kini informasi tersebar di ruang digital

yang tak kenal batas. Dunia maya menjadi medan pertempuran baru di mana peretas dan mata-mata *cyber* saling berburu informasi. Aneka perangkat digital dari telepon genggam hingga satelit canggih melengkapi setiap misi, menjadikan pengumpulan data makin efisien dan terarah. Namun, ada tantangan tersendiri di dalam kekayaan informasi ini, yaitu terlalu banyak suara yang harus disaring untuk menemukan kebenaran yang dibutuhkan.

Memasuki milenium baru, terutama setelah peristiwa 11 September 2001, terorisme tidak lagi dipandang sebelah mata sebagai ancaman domestik yang bisa diabaikan. Serangan tersebut mengguncang kesadaran global akan bahaya terorisme transnasional (Hoffman, 2006). Respon dari negara-negara besar adalah memperkuat peran intelijen dalam upaya memerangi terorisme. Dalam kerangka baru anti-terorisme global, lembaga-lembaga intelijen menjalin kerjasama lintas batas negara, berbagi informasi, dan menyusun strategi kontra-terorisme secara komprehensif. Ekses dari hal ini adalah pembentukan jaringan intelijen internasional yang saling terkait dan mendukung dalam memerangi musuh bersama yang tak terlihat.

Di sisi lain, penguatan kedudukan intelijen di era ini mengundang kritik terkait pelanggaran privasi dan kebebasan sipil. Operasi pengawasan yang dilakukan di ruang digital seringkali menimbulkan perdebatan tentang batas-batas kebebasan individu. Bagi banyak orang, peran intelijen yang mengumpulkan data secara masif dianggap sebagai ancaman terhadap demokrasi dan hak asasi manusia. Tantangan moral dan etis ini terus menjadi perdebatan sengit di berbagai forum internasional (Miller, Regan, & Walsh, 2022). Namun, di balik kontroversi tersebut, intelijen tetap menjadi komponen krusial dalam menjaga stabilitas dan keamanan internasional.

Tidak bisa dipungkiri bahwa ancaman global masa kini memerlukan pendekatan multidimensional yang melibatkan kolaborasi berbagai elemen dan aktor di dalam dan di luar ranah pemerintahan. Penggunaan kekuatan keras seringkali tidak memadai dalam menghadapi serbuan ancaman terorisme dan kelompok radikal yang memiliki kecepatan adaptasi tinggi. Di sinilah inovasi dalam intelijen strategis memainkan

peran krusial. Pemahaman mendalam mengenai kultur, ideologi, dan psikologi menjadi faktor kunci dalam meracik strategi yang efektif. Dari pemetaan jaringan kelompok ekstremis hingga pelaksanaan operasi infiltrasi untuk mendapatkan data sahih.

Menariknya, dalam perkembangan dunia intelijen dewasa ini, perhatian juga diberikan kepada keterlibatan masyarakat umum sebagai bagian dari upaya kontra-terorisme (Briggs, 2010). Konsep masyarakat sipil yang memiliki kesadaran keamanan di sekitar lingkungannya turut mengajak individu-individu untuk proaktif dalam memerangi terorisme. Bentuk kerjasama ini diharapkan dapat mempersempit ruang gerak bagi kelompok teroris untuk mencari basis dukungan dan simpatisan.

Di dalam ranah politik global, intelijen juga menjadi alat sikap kekuasaan. Negara-negara besar menggunakan informasi intelijen tidak hanya sebagai langkah defensif, tetapi juga ofensif dalam mempengaruhi kebijakan dan ekonomi negara lain (Lowenthal, 2017). Fenomena ini menimbulkan lanskap baru di mana persaingan untuk mendapatkan dominasi informasi menjadi permainan geopolitik yang rumit. Beberapa negara terlibat dalam operasi cyber untuk mencapai tujuan politik mereka, yang sering disebut sebagai perang dingin digital (Armis, 2025. Dalam era di mana informasi adalah senjata, keberhasilan strategi intelijen menjadi penentu bagi sebuah negara dalam mempertahankan eksistensinya di tengah percaturan global.

Intelijen juga mengalami transformasi dalam pendekatannya terhadap ancaman ancaman alam seperti pandemi global. Krisis kesehatan yang melanda dunia, seperti yang disebabkan oleh COVID-19, memperlihatkan bagaimana intelijen medis dan bio-sekuriti memainkan peran signifikan dalam deteksi dini serta mitigasi ancaman yang tidak hanya berisiko menelan korban jiwa tetapi juga mengguncang stabilitas sosial dan ekonomi (Bahtiar, Purwadianto & Juwono, 2021).

Laporan intelijen yang akurat dan cepat menjadi komoditas berharga yang memandu para pengambil keputusan dalam merumuskan kebijakan publik yang tepat dan efektif. Di saat krisis, sinergi antara lembaga intelijen dengan instansi kesehatan serta otoritas lain menjadi

kian penting, mengingat dampak multidimensional dari krisis yang melibatkan banyak aspek kehidupan manusia dan lingkungan.

Begitu juga dengan ancaman perubahan iklim. Intelijen diharapkan dapat menjalankan peran baru sebagai pengawas tren-tren klimatologis serta dampak keberlanjutannya terhadap ketahanan pangan, keamanan energi, dan migrasi massal. Tugas ini tidak ringan, menandakan bagaimana intelijen harus terus berkembang mengikuti dinamika zaman yang penuh tantangan (Weissmann, 2025).

Dengan segala perubahan ini, satu hal yang tetap menjadi relevan adalah kebutuhan akan agen-agen lapangan yang berani dan berdedikasi. Di balik teknologi canggih dan analisis data yang mendalam, operasi intelijen sejatinya masih memerlukan sentuhan manusiawi yang khas. Mata-mata yang bekerja di lapangan, senyap dalam senyuman dan percakapan ringan, berperan menjalin kontak dan membangun jaringan informasi dari sumber-sumber yang dipercaya.

Teknologi dapat memudahkan dan melengkapi, tetapi tidak bisa sepenuhnya menggantikan pentingnya kehadiran manusia yang dapat menilai situasi secara kontekstual dan memberikan laporan yang paletnya mewarnai kebijakan-kebijakan dunia. Di sinilah letak tantangan bagi lembaga-lembaga intelijen di seluruh dunia dalam meramu campuran yang sempurna antara teknisi dan agen lapangan, antara data statistik dan naluri manusia (Mulya, 2025).

Kehidupan dunia intelijen di tengah era baru yang kian kompleks dan menantang ini terus mengingatkan kita bahwa keamanan yang kita nikmati hari ini adalah hasil dari kerja keras, pengorbanan, dan perjuangan yang tidak kasatmata. Agensi intelijen berdiri sebagai garda terdepan dalam menjaga tanah air dan dunia dari ancaman-ancaman yang bersembunyi di bayang-bayang globalisasi.

Dengan sikap tetap waspada dan berusaha memahami perkembangan-perkembangan terkini, tugas penting intelijen sebagai alat kekuasaan global semakin penting dan menantang. Dunia baru ini, dengan segala musuh tak kasatmata yang ada, memerlukan agen-agen intelijen dan strategi yang tidak hanya berani dan cerdas, tetapi juga bersikap luwes dan adaptif menghadapi segala macam ancaman yang

bisa datang kapan saja. Intelijen, dalam wajah barunya, adalah pilar pertahanan negara yang harus tetap siap menghadapi segala sesuatu yang penuh kemungkinan di masa depan.

### 1.3.1 Peran Strategis dan Dinamika Evolusinya

Dalam arsitektur keamanan internasional kontemporer, intelijen tidak lagi hanya menjadi penjara informasi rahasia yang dikelola oleh negara untuk keperluan kebijakan luar negeri. Sebaliknya, ia telah menjadi instrumen kekuasaan global yang memainkan peran strategis yang sangat menentukan. Intelijen, khususnya di abad ke-21, telah mengalami evolusi signifikan, menjadi komponen yang fundamental dalam operasi *soft power* dan *hard power*, serta berfungsi sebagai penghubung penting dalam diplomasi internasional dan perang non-konvensional (Bury & Chertoff, 2020).

Peran strategis intelijen kini tidak hanya terbatas pada pengumpulan dan analisis informasi. Dalam dinamika global yang cepat berubah, intelijen telah menjadi bagian integral dari pembuatan keputusan kebijakan (Lowenthal, 2017). Dengan kecepatan perkembangan teknologi informasi, alat dan metode intelijen telah beradaptasi, memungkinkan informasi dieksploitasi hampir secara *real-time* untuk memberikan keunggulan kompetitif dalam arena global. Misalnya, dalam pengambilan keputusan krisis, seperti langkah-langkah yang diambil untuk menanggapi tindakan agresif oleh negara lain, analisis dan laporan intelijen sering kali menjadi acuan utama.

Di kehidupan sehari-hari, kita bisa melihat contoh nyata dari penggunaan intelijen melalui penanganan pandemi COVID-19. Berbagai negara menggunakan kemampuan intelejen mereka untuk melacak penyebaran virus, memprediksi pola penyebaran lebih lanjut, dan memahami kebijakan negara lain dalam merespons pandemik, termasuk Indonesia (Bahtiar, Purwadianto, Juwono, 2021). Informasi ini menjadi krusial untuk mengoordinasikan respons internasional dan mengamankan ketersediaan vaksin. Kecerdasan buatan dan analitik data menjadi alat yang tidak terpisahkan dalam mengolah *big data* guna memetakan tren infeksi serta mengantisipasi terjadinya gelombang baru.

Dinamika evolusi dari peran intelijen secara jelas terlihat dari bagaimana perannya bergeser dari sekadar pendukung operasi militer menjadi perantara dalam kebijakan ekonomi dan sosial. Sebagai contoh, *Central Intelligence Agency* (CIA) di Amerika Serikat atau *Military Intelligence Section* 6 (MI6) di Inggris, kini semakin berfokus pada analisis ekonomi dan sosial selain dari tujuan tradisionalnya seperti identifikasi ancaman militer. Mereka tidak hanya menganalisis situasi geopolitik, tapi juga fenomena global seperti perubahan iklim, migrasi manusia, dan krisis ekonomi, yang semuanya memiliki implikasi keamanan.

Lebih jauh, perangkat dan kemampuan intelijen telah berkembang secara signifikan dengan mengadopsi teknologi-teknologi baru seperti penginderaan jarak jauh, satelit mata-mata, dan teknologi siber yang canggih (Atkinson, 2024). Evolusi ini memungkinkan aktivitas pengumpulan intelijen dilakukan secara lebih efisien dan dalam jangkauan yang lebih luas. Peningkatan penggunaan teknologi penginderaan jauh dan satelit memungkinkan pengawasan dan pengintaian terhadap area geografis yang luas dan sulit dijangkau secara fisik, seperti di wilayah perbatasan.

Teknologi siber yang terus berkembang telah membawa intelijen ke ranah perang maya atau *cyberwarfare*. Serangan siber pada infrastruktur kritis dapat melumpuhkan pertahanan suatu negara, dan laporan-laporan intelijen siber menjadi elemen vital dalam melindungi dari ancaman demikian (Clarke & Knake, 2010). Contohnya adalah serangan siber yang menimpa jaringan energi dan komunikasi Ukraina sebelum perang Rusia-Ukraina. Serangan ini menunjukkan perlunya ketahanan siber yang kuat dan penggunaan intelijen siber untuk mengantisipasi serta menetralkan ancaman sebelum terjadi serangan fisik.

Dinamika evolusi intelijen juga melibatkan kerjasama internasional yang lebih erat dan pertukaran informasi lintas batas. Organisasi internasional seperti Interpol dan Europol menjadi platform di mana berbagai agensi intelijen dapat berbagi informasi untuk melacak aktivitas terorisme, kejahatan terorganisir, dan ancaman global lainnya (Yusuf dkk, 2025). Kerjasama ini juga melibatkan latihan bersama dan pembangunan kapasitas di antara negara-negara yang seringkali

menghadapi ancaman bersama. Namun, kerjasama ini tidak serta merta terjadi tanpa tantangan. Kepercayaan, kerahasiaan, dan pertimbangan politik menjadi hambatan yang perlu diatasi untuk memungkinkan kolaborasi intelijen yang efektif.

Kita juga tak bisa mengesampingkan peran besar intelijen dalam perang melawan terorisme. Setelah peristiwa 11 September 2001, investasi besar-besaran dilakukan oleh banyak negara, terutama Amerika Serikat dalam meningkatkan kapabilitas intelijen mereka untuk menghadapi ancaman aktor non-negara yang tidak kasat mata ini (Clarke, 2004). Operasi pengejaran dan penangkapan para pemimpin teroris, sebagaimana yang terjadi pada penangkapan Osama bin Laden, menunjukkan signifikansi operasi intelijen dalam mencapai tujuan strategis dalam perang terhadap teror.

Peran strategis dan dinamika evolusi intelijen sebagai alat kekuasaan global tidak dapat diremehkan. Dari menangani ancaman fisik hingga risiko siber, dari membangun kepercayaan internasional hingga menghadapi fenomena global, intelijen terus-menerus bertransformasi untuk menjawab kebutuhan zaman. Dalam konteks ini, publik mungkin jarang menyadari besarnya peran intelijen dalam kehidupan sehari-hari, tetapi pengaruhnya menyentuh aspek berbagai kebijakan pemerintah yang berdampak pada kesejahteraan sosial, keamanan, dan perkembangan global secara langsung dan tidak langsung. Peran ini memastikan bahwa negara selalu berada selangkah di depan dalam menghadapi ketidakpastian dunia yang terus berubah, menjadikannya sebuah elemen yang esensial dalam memegang kendali atas peta kekuatan global.

### 1.3.2 Batas Tipis antara Perlindungan dan Pengendalian

Dalam era modern ini, dunia menghadapi berbagai tantangan yang tidak seperti sebelumnya. Intelijen, yang awalnya dirancang sebagai mekanisme perlindungan, telah berkembang menjadi salah satu alat kekuasaan global yang paling signifikan. Pada sub bab ini, kita akan mengeksplorasi bagaimana intelijen berfungsi baik sebagai pelindung maupun sebagai sarana pengendalian dalam arsitektur keamanan

internasional, serta implikasi yang timbul dari peran gandanya di masyarakat.

Pada hakikatnya, intelijen berfungsi untuk mengumpulkan informasi yang dapat membantu negara memahami dan merespons ancaman yang muncul. Ini mengenai menjaga keamanan nasional dan memprediksi potensi ancaman sebelum mereka berkembang menjadi krisis besar. Di era di mana informasi merupakan salah satu komoditas paling berharga, kemampuan untuk mengambil dan menganalisis data dengan cepat memberikan negara-negara keunggulan yang tak ternilai (Bury & Chertoff, 2020).

Namun, seiring dengan meningkatnya kemampuan teknologi, batas antara perlindungan dan pengendalian semakin kabur. Pada satu sisi, intelijen harus memantau ancaman eksternal seperti terorisme, spionase, dan serangan dunia maya. Pada sisi lain, alat yang sama dapat digunakan untuk memantau warga negara sendiri, yang sering kali melanggar hak privasi individu (Miller & Walsh, 2022). Di sinilah letak paradoks modern: upaya untuk melindungi malah dapat berujung pada upaya untuk mengendalikan.

Contoh nyata dari dilema ini adalah pengawasan massal yang dilakukan oleh beberapa negara dengan dalih keamanan nasional. Program pengawasan yang diungkapkan Edward Snowden, misalnya, menunjukkan sejauh mana intelijen dapat digunakan untuk memantau komunikasi pribadi. Di Amerika Serikat, Badan Keamanan Nasional (NSA) terlibat dalam pengumpulan metadata telepon dan komunikasi elektronik dari jutaan orang, baik di dalam negeri maupun internasional (Em/al, 2019). Meski dimaksudkan untuk mengidentifikasi dan mencegah serangan teroris, kebijakan ini menimbulkan kritik tajam karena dianggap melanggar kebebasan sipil.

Begitu juga dengan teknologi pengenalan wajah yang kini banyak digunakan oleh pemerintah dan perusahaan swasta. Meskipun dapat meningkatkan keamanan publik dengan mengidentifikasi pelaku kriminal dalam kerumunan, praktik ini juga menimbulkan kekhawatiran tentang penyalahgunaan data dan hak privasi. Di beberapa kota besar di dunia, teknologi ini telah digunakan untuk memantau pergerakan

individu sehari-hari, yang ketika jatuh ke tangan yang salah, dapat menjadi alat penindasan politik.

Di sisi lain, intelijen memiliki fungsi penting dalam mencegah aksi terorisme yang mengancam stabilitas global. Kolaborasi antar lembaga intelijen internasional telah berhasil menggagalkan sejumlah rencana serangan sebelum sempat dieksekusi. Kasus penangkapan teroris di Eropa yang terbukti memiliki jaringan dengan kelompok ekstrimis internasional menunjukkan efektivitas kerja sama intelijen yang baik. Namun, pertanyaannya tetap: sejauh mana kita bisa mempercayai sistem yang begitu kuat tanpa mengorbankan kebebasan individu?

Dunia digital telah memudahkan aktivitas pengumpulan intelijen, namun juga telah membuat ancaman menjadi lebih kompleks. Serangan siber, misalnya, kini dapat dilakukan oleh aktor negara maupun non-negara untuk mencuri data sensitif atau melumpuhkan infrastruktur penting. Insiden peretasan terhadap institusi besar seperti yang dialami oleh pemerintahan Ukraina dan disalahkan pada aktor eksternal menunjukkan kompleksitas ancaman modern ini. Dalam hal ini, intelijen bukan hanya menjadi alat protektif tetapi juga senjata strategis dalam peperangan era baru di dunia maya.

Penerapan intelijen bukan hanya masalah teknis, tetapi juga moral dan etika. Kebijakan dan operasi yang dijalankan harus dibarengi dengan pertimbangan etis yang matang agar tidak melampaui batas. Inovasi dalam teknologi intelijen harus disertai dengan regulasi yang kuat dan transparan untuk mencegah penyalahgunaan kekuasaan (Mulya, 2025).

Pengawasan publik dan mekanisme *check and balance* yang efektif antara lembaga intelijen, pemerintah, dan masyarakat harus terus dilakukan untuk menjamin bahwa kebijakan yang diambil berada dalam koridor demokrasi. Salah satu contohnya adalah mekanisme *oversight* di beberapa negara maju, di mana lembaga investigasi independen dibentuk untuk menilai dan mengawasi operasi intelijen. Namun, tak dapat dipungkiri, pemusatan data yang ada hingga saat ini membuat banyak pihak khawatir akan potensi kebocoran dan penyalahgunaannya. Di mana batasan antara privasi individu dan kebutuhan keamanan

nasional? Bagaimana kita dapat memastikan bahwa teknologi intelijen lebih bersifat melindungi daripada mengancam kehidupan sipil?

Peristiwa terbaru di negara-negara seperti Tiongkok menunjukkan bagaimana intelijen dapat digunakan sebagai alat pengendalian sosial yang ekstrim. Sistem kredit sosial yang diterapkan menggunakan teknologi pengawasan untuk memantau aktivitas penduduk dan memberikan "skor" berdasarkan perilaku mereka (IPDF, 2019). Sanksi sosial dan ekonomi dapat dikenakan pada individu berdasarkan skor ini, sehingga menimbulkan banyak kritik internasional tentang pelanggaran hak asasi manusia.

Tantangan ini mengingatkan kita bahwa meskipun intelijen adalah alat penting dalam menjaga keamanan, penggunaannya harus tetap dibatasi oleh prinsip-prinsip yang menjamin penghormatan terhadap kebebasan dan hak asasi manusia. Inisiatif untuk menciptakan standar internasional dan kerangka kerja yang mengatur penggunaan teknologi pengawasan dapat membantu menjembatani kesenjangan ini. Kesepakatan global seperti yang dirumuskan dalam Deklarasi Privasi Internasional dapat menjadi langkah awal yang penting.

Ujung tombak dari perdebatan ini adalah bagaimana kita memandang peran negara dalam melindungi warga negara sembari menghormati otonomi individu. Pembentukan kebijakan yang bijaksana dan berkelanjutan harus melibatkan diskusi antara pemerintah, masyarakat sipil, dan komunitas internasional untuk menemukan keseimbangan antara keamanan dan kebebasan. Ke depan, transparansi dan rasa saling percaya harus menjadi fondasi hubungan antara intelijen dan publik yang dilayani.

Kesadaran publik tentang isu ini lebih penting dari sebelumnya, karena hanya dengan pengetahuan dan keterlibatan aktif, masyarakat dapat memainkan peran mereka dalam memastikan bahwa perangkat intelijen berfungsi untuk melayani kepentingan bersama. Dalam dunia yang semakin terhubung dan tidak stabil ini, kita harus terus waspada terhadap batas tipis antara perlindungan dan pengendalian, serta menemukan cara paling efektif untuk beradaptasi dengan perubahan yang cepat tanpa kehilangan esensi kemanusiaan kita.