

## Kontraintelijen Pada Era Kontemporer Dalam Mencegah Ancaman Intelijen Asing dan Implikasinya Terhadap Ketahanan Wilayah Ibu Kota Nusantara di Kalimantan Timur

*Stanislaus Riyanta<sup>1</sup>, Diah Ayu Permatasari<sup>2</sup>*

<sup>1</sup>Universitas Indonesia

<sup>2</sup>Universitas Bhayangkara Jakarta Raya

\*korespondensi email: stanislaus@ui.ac.id

Dikirim: 4-8-2025 .Direvisi: 13-08-2025, Diterima: 24-8-2025

### **ABSTRACT**

*This article examines the crucial role of counterintelligence in supporting early detection and prevention of foreign threats in the contemporary era, as well as its implications for the resilience of the Nusantara Capital Region (IKN). This study aims to comprehensively analyze the definition, functions, and implications of counterintelligence for national resilience in the modern era, and to identify the challenges faced in its implementation. Through a qualitative literature review approach, this study analyzes the definitions, functions, and evolution of counterintelligence, as well as its adaptation to modern challenges such as technological advancements, resource limitations, and ethical dilemmas. The analysis results indicate that counterintelligence, with key components such as prevention, detection, deception, and counterespionage, plays a vital role in enhancing national security, supporting strategic decision-making, and preventing financial losses while building public trust. It is concluded that counterintelligence is an integral element of the national resilience strategy that requires continuous adaptation, inter-agency collaboration, transparency, and accountability to protect the Nusantara Capital Region from evolving threats.*

**Keywords:** Counterintelligence; National Resilience; National Threat; Nusantara Capital.

### **ABSTRAK**

Artikel ini mengkaji peran krusial kontraintelijen dalam mendukung fungsi deteksi dini dan pencegahan ancaman asing di era kontemporer, serta implikasinya terhadap ketahanan wilayah Ibu Kota Nusantara (IKN). Penelitian ini bertujuan untuk menganalisis secara komprehensif definisi, fungsi, dan implikasi kontraintelijen terhadap ketahanan nasional di era modern, serta mengidentifikasi tantangan yang dihadapi dalam pelaksanaannya. Melalui pendekatan studi literatur kualitatif, penelitian ini menganalisis definisi, fungsi, dan evolusi kontraintelijen, serta adaptasinya terhadap tantangan modern seperti kemajuan teknologi, keterbatasan sumber daya, dan dilema etika. Hasil analisis menunjukkan bahwa kontraintelijen, dengan komponen utama seperti pencegahan, deteksi, penipuan, dan kontraespionase, berperan penting dalam meningkatkan keamanan nasional, mendukung pengambilan keputusan strategis, serta mencegah kerugian finansial dan membangun kepercayaan publik. Disimpulkan bahwa kontraintelijen merupakan elemen integral dalam strategi ketahanan nasional yang memerlukan adaptasi berkelanjutan, kolaborasi antar lembaga, transparansi, dan akuntabilitas untuk melindungi Ibu Kota Nusantara dari ancaman yang terus berkembang.

**Kata kunci:** Kontraintelijen; Ketahanan Nasional; Ancaman Nasional; Ibu Kota Nusantara.

## PENGANTAR

Dalam konflik yang berlarut-larut antara Iran dan Israel, peran intelijen telah menjadi sangat sentral, dengan kedua belah pihak secara aktif terlibat dalam operasi rahasia untuk mendapatkan keuntungan strategis. Israel, terutama melalui Mossad, telah secara efektif mengeksplorasi kerentanan dalam struktur intelijen Iran, yang diperparah oleh persaingan internal, kerapuhan rezim, dan lingkungan geopolitik yang tegang (Serscikov, 2024, hlm. 89, 92). Operasi-operasi ini mencakup sabotase fasilitas nuklir, seperti serangan Stuxnet pada tahun 2009, dan pembunuhan ilmuwan nuklir terkemuka Iran, Mohsen Fakhrizadeh pada tahun 2020, yang menunjukkan tingkat kecanggihan dan kompleksitas yang tinggi dalam operasi intelijen Israel (Serscikov, 2024, hlm. 90, 98).

Sebaliknya, meskipun intelijen Iran telah mencapai beberapa keberhasilan dalam merekrut agen-agen penting: Seperti mantan menteri energi Israel Gonen Segev, mereka sering kali menunjukkan kurangnya kecanggihan di luar Timur Tengah dalam menghadapi tantangan dan menahan tekanan intens dari badan intelijen kelas satu (Serscikov, 2024, hlm. 90, 102). Dinamika ini menyoroti bahwa intelijen bukan hanya alat pengumpulan informasi, tetapi juga instrumen penting untuk memanipulasi persepsi, menguras sumber daya, dan mengganggu proses pengambilan keputusan lawan, yang secara signifikan membentuk jalannya konflik yang sebagian besar bersifat *klandestin* ini (Serscikov, 2024, hlm. 103-104).

Kontraintelijen berfungsi sebagai garis pertahanan pertama yang melindungi informasi sensitif dan operasi rahasia dari pengintaian dan sabotase. Operasi ini mencakup tindakan defensif dan ofensif, yang

dirancang untuk mendeteksi, mencegah, dan mengatasi kegiatan intelijen yang merugikan. Tujuan utama dari operasi kontraintelijen adalah melindungi sumber daya dan informasi vital bagi keamanan nasional, termasuk pengumpulan intelijen tentang aktivitas musuh dan penggagalan operasi intelijen yang sedang berlangsung (Lowenthal, 2017).

Operasi kontraintelijen dapat dibagi menjadi beberapa kategori, seperti pencegahan, deteksi, penggagalan, dan rekrutmen informan. Setiap kategori memiliki teknik dan metode yang berbeda, termasuk pengawasan fisik dan elektronik, infiltrasi, serta penggunaan penyamaran. Namun, pelaksanaan operasi ini menghadapi tantangan, seperti perkembangan teknologi informasi yang mengubah cara intelijen dikumpulkan dan dipertukarkan, serta keterbatasan anggaran yang dapat membatasi efektivitas operasi (Wettering, 2000).

Lanskap geopolitik yang dinamis dan penuh ketidakpastian, peran intelijen menjadi semakin sentral sebagai fondasi bagi keamanan nasional dan, pada gilirannya, ketahanan nasional. Intelijen, sebagai proses pengumpulan, analisis, dan diseminasi informasi strategis, tidak hanya berfungsi untuk mengidentifikasi ancaman dan peluang, tetapi juga menjadi instrumen krusial dalam membentuk kebijakan pertahanan dan luar negeri. Keamanan nasional, yang merupakan prasyarat bagi eksistensi dan kemajuan suatu negara, sangat bergantung pada efektivitas operasi intelijen dalam melindungi kedaulatan, integritas wilayah, dan kepentingan vital dari berbagai ancaman, baik dari aktor negara maupun non-negara. Lebih jauh lagi, keamanan nasional yang kokoh akan secara langsung berkontribusi pada penguatan ketahanan nasional, yaitu kemampuan suatu bangsa untuk menghadapi, beradaptasi, dan

pulih dari berbagai guncangan dan tantangan, memastikan keberlanjutan pembangunan dan kesejahteraan masyarakat dalam jangka panjang.

Dalam konteks pembangunan dan pemindahan Ibu Kota Nusantara (IKN) sebagai pusat pemerintahan dan simbol ketahanan nasional Indonesia, peran kontraintelijen menjadi semakin krusial. IKN, dengan segala aset strategis, infrastruktur vital, dan informasi sensitif yang akan terkonsentrasi di dalamnya, secara inheren akan menjadi target utama bagi berbagai ancaman intelijen asing, baik dari aktor negara maupun non-negara. Ancaman ini dapat berupa spionase untuk mencuri rahasia negara, sabotase terhadap infrastruktur kritis, subversi untuk mengganggu stabilitas sosial dan politik, hingga kampanye disinformasi yang bertujuan merusak citra dan kepercayaan publik terhadap pemerintah. Oleh karena itu, kontraintelijen tidak hanya berfungsi sebagai mekanisme pertahanan pasif, melainkan sebagai elemen proaktif yang esensial untuk memastikan keamanan, keberlanjutan pembangunan, dan ketahanan IKN dari segala bentuk intervensi dan eksloitasi yang merugikan kepentingan nasional. Tanpa sistem kontraintelijen yang kuat dan adaptif, IKN akan rentan terhadap penetrasi yang dapat membahayakan kedaulatan, integritas, dan masa depan bangsa.

Penelitian ini bertujuan untuk menganalisis secara komprehensif definisi, fungsi, dan implikasi kontraintelijen terhadap ketahanan nasional di era kontemporer, serta mengidentifikasi tantangan yang dihadapi dalam pelaksanaannya. Urgensi penelitian ini terletak pada semakin kompleksnya ancaman kontemporer seperti serangan siber dan disinformasi, yang menuntut pemahaman mendalam tentang peran kontraintelijen

sebagai garda terdepan dalam menjaga stabilitas dan integritas negara, sekaligus mengisi kesenjangan pengetahuan dan kebijakan yang ada. Pemilihan Ibu Kota Nusantara (IKN) sebagai lokus penelitian sangat strategis karena IKN, sebagai pusat pemerintahan dan simbol ketahanan, secara inheren menjadi target utama ancaman intelijen asing, menjadikan kontraintelijen sebagai subjek krusial untuk melindungi aset vital dan proses pengambilan keputusan. Untuk mencapai tujuan tersebut, penelitian ini menggunakan metode penelitian kualitatif dengan sumber data dari studi kepustakaan yang sangat sesuai untuk mengkaji berbagai sumber primer dan sekunder dari para ahli di bidang intelijen, keamanan, dan ketahanan nasional. Studi kepustakaan ini memungkinkan interpretasi mendalam terhadap konsep dan praktik kontraintelijen dalam konteks historis dan kontemporer, serta mendukung pengembangan kerangka teoritis yang kuat untuk merumuskan rekomendasi kebijakan yang relevan.

## **PEMBAHASAN**

Bagian pembahasan ini akan menguraikan secara komprehensif definisi, fungsi, dan implikasi kontraintelijen terhadap ketahanan wilayah Ibu Kota Nusantara (IKN) di era modern, serta mengidentifikasi berbagai tantangan yang dihadapi dalam pelaksanaannya. Dimulai dengan menelusuri sejarah singkat kontraintelijen, kita akan melihat bagaimana praktik ini telah berevolusi dari zaman kuno hingga era kontemporer, beradaptasi dengan perubahan lanskap ancaman global yang kini juga menyasar entitas strategis seperti IKN. Selanjutnya, pembahasan akan mendalam berbagai definisi kontraintelijen dari para ahli, mengidentifikasi

fungsi-fungsi spesifiknya, dan menganalisis strategi defensif maupun ofensif yang diterapkan dalam konteks perlindungan IKN. Terakhir, bagian ini akan mengkaji komponen-komponen kunci kontraintelijen, urgensi dalam menjaga keamanan informasi dan aset-aset vital IKN, serta manfaat yang diberikannya, sebelum membahas konsep operasi kontraintelijen dan tantangan etika yang menyertainya khususnya dalam menjaga integritas dan keberlanjutan IKN.

### Sejarah Singkat Kontraintelijen

Kontraintelijen adalah upaya untuk melindungi informasi dan operasi dari pengintaian dan sabotase oleh musuh. Sejarah kontraintelijen dapat ditelusuri kembali ke zaman kuno, tetapi berkembang pesat selama abad ke-20, terutama selama Perang Dunia I dan II. Kontraintelijen telah ada sejak zaman kuno, ketika negara-negara menggunakan mata-mata untuk mengumpulkan informasi tentang musuh mereka. Namun, praktik yang lebih terorganisir mulai muncul pada abad ke-19. Salah satu contoh awal adalah pembentukan Bureau of Military Intelligence di Inggris pada tahun 1882, yang bertujuan untuk mengawasi aktivitas mata-mata asing (Hoffman, 2006).

Selama Perang Dunia I, kontraintelijen menjadi semakin penting. Negara-negara terlibat dalam perang total, di mana informasi menjadi senjata yang sangat berharga. Inggris membentuk MI5 (Military Intelligence, Section 5) untuk melawan spionase Jerman. MI5 berhasil mengungkap jaringan spionase Jerman di Inggris, yang dikenal sebagai “*The Black Hand*” (Andrew, 2009).

Perang Dunia II melihat perkembangan yang signifikan dalam kontraintelijen. Di Amerika Serikat, *Office of Strategic Services*

(OSS) didirikan pada tahun 1942 untuk mengumpulkan intelijen dan melakukan operasi rahasia. OSS memainkan peran penting dalam mengungkap rencana musuh dan melindungi informasi strategis (Richelson, 2007). Di Eropa, kontraintelijen Jerman, Abwehr, berusaha untuk mengidentifikasi dan menghancurkan jaringan intelijen Sekutu, tetapi sering kali gagal karena infiltrasi dan pengkhianatan di dalamnya (Mahnken, 2007).

Perang Dingin (1947-1991) ditandai oleh ketegangan antara blok Barat yang dipimpin oleh Amerika Serikat dan blok Timur yang dipimpin oleh Uni Soviet. Dalam konteks ini, kontraintelijen menjadi alat penting untuk melindungi informasi sensitif dan mencegah infiltrasi musuh. Di Amerika Serikat, Central Intelligence Agency (CIA) dibentuk pada tahun 1947 dan menjadi lembaga utama dalam pengumpulan intelijen dan operasi kontraintelijen (Prados, 2006).

CIA mengembangkan berbagai teknik untuk melawan spionase Soviet, termasuk pengawasan, infiltrasi, dan operasi rahasia. Salah satu operasi terkenal adalah “*Operation CHAOS*,” yang bertujuan untuk mengawasi dan mengganggu gerakan anti-perang di dalam negeri (Richelson, 2007). Selama periode ini, banyak kasus infiltrasi yang mengkhawatirkan terjadi. Salah satu yang paling terkenal adalah kasus Julius dan Ethel Rosenberg, yang dieksekusi pada tahun 1953 karena didakwa memberikan informasi nuklir kepada Uni Soviet. Kasus ini menunjukkan betapa seriusnya ancaman spionase terhadap keamanan nasional Amerika Serikat (Braman, 2006).

Di sisi lain, Uni Soviet juga mengembangkan program kontraintelijen yang kuat melalui KGB (Komitet Gosudarstvennoy Bezopasnosti). KGB berfokus pada

pengawasan terhadap warga negara dan pengumpulan informasi tentang musuh, serta melakukan operasi untuk mengganggu aktivitas intelijen Barat (Andrew, 2009).

Dengan berakhirnya Perang Dingin pada awal 1990-an, fokus kontraintelijen mulai beralih. Ancaman baru muncul, termasuk terorisme internasional dan proliferasi senjata pemusnah massal. Lembaga-lembaga intelijen di seluruh dunia mulai beradaptasi dengan tantangan baru ini. Di Amerika Serikat, setelah serangan 11 September 2001, kontraintelijen menjadi lebih terintegrasi dengan upaya keamanan dalam negeri (Zegart, 2007).

Sejarah kontraintelijen pasca Perang Dunia II menunjukkan evolusi yang signifikan dalam strategi dan teknik yang digunakan untuk melindungi informasi dan mencegah infiltrasi. Dari ketegangan Perang Dingin hingga tantangan baru di era modern, kontraintelijen tetap menjadi komponen penting dalam menjaga ketahanan nasional.

Di era modern, kontraintelijen telah berkembang untuk menghadapi ancaman yang lebih kompleks, termasuk serangan siber dan disinformasi. Menurut Putter (2025), perang kognitif dan kontraintelijen menjadi elemen penting dalam strategi keamanan di Afrika. Dalam konteks ini, negara-negara harus mengembangkan kemampuan untuk melawan propaganda dan disinformasi yang dapat merusak kepercayaan publik terhadap institusi pemerintah.

### **Definisi, Fungsi dan Strategi Kontraintelijen**

Kontraintelijen dapat didefinisikan sebagai kegiatan yang dilakukan untuk mendekripsi, mencegah, dan mengatasi operasi intelijen yang dilakukan oleh pihak asing atau kelompok yang berpotensi merugikan keamanan nasional. Menurut Prunckun

(2019), kontraintelijen mencakup berbagai taktik, termasuk pengawasan, infiltrasi jaringan musuh, operasi penipuan, dan perlindungan informasi sensitif. Dalam konteks ini, kontraintelijen tidak hanya berfungsi sebagai alat defensif, tetapi juga sebagai alat ofensif untuk mengganggu dan melemahkan kemampuan musuh.

Sherman Kent (1949) mendefinisikan kontraintelijen sebagai “pengetahuan yang diperlukan untuk perlindungan dan pelestarian kekuatan militer, ekonomi, dan produktif Amerika Serikat, termasuk keamanan Pemerintah dalam urusan domestik dan luar negeri, terhadap atau dari spionase, sabotase, subversi, dan semua tindakan ilegal lainnya yang dirancang untuk melemahkan atau menghancurkan Amerika Serikat” (Barnea, 2020). Pada pengertian lain Van Cleave menyatakan bahwa kontraintelijen mencakup kegiatan yang dilakukan untuk mencegah atau menggagalkan operasi intelijen musuh, termasuk spionase, sabotase, dan aktivitas clandestine lainnya yang dilakukan oleh pemerintah, organisasi, atau individu asing (Putter, 2024).

Dov Bachmann (et all) menyatakan bahwa kontraintelijen berfungsi untuk “mengidentifikasi, menilai, menetralkan, dan mengeksplorasi ancaman terhadap keamanan nasional yang ditimbulkan oleh aktivitas intelijen musuh” (Bachmann, Putter, & Duczynski, 2023).

Dari berbagai definisi tersebut dapat disimpulkan sebuah definisi dari kontraintelijen yaitu serangkaian kegiatan defensif maupun ofensif yang bertujuan untuk mendekripsi, mencegah, dan mengatasi operasi intelijen yang dilakukan oleh pihak asing atau kelompok yang berpotensi merugikan keamanan nasional. Kegiatan kontraintelijen

mencakup berbagai taktik, seperti pengawasan, infiltrasi jaringan musuh, operasi penipuan, dan perlindungan informasi sensitif.

Kontraintelijen dijabarkan mempunyai fungsi-fungsi yang spesifik. Fungsi-fungsi tersebut antara lain kontraintelijen sebagai fungsi strategis, yang digunakan untuk melindungi informasi dan operasi intelijen dari ancaman musuh. Ini mencakup pengumpulan informasi tentang aktivitas intelijen musuh dan upaya untuk mengganggu atau menghentikan operasi mereka (Reed & Mc Ivor, 2005). Kontraintelijen juga mempunyai fungsi perlindungan dalam konteks ini, kontraintelijen dipandang sebagai proses yang bertujuan untuk melindungi organisasi dari pengintaian dan sabotase. Ini melibatkan tindakan pencegahan dan respons terhadap ancaman yang dapat merusak keamanan nasional (Prunckun, 2011).

Fungsi kontraintelijen selanjutnya adalah keamanan internal, yang bertujuan untuk mendekripsi dan mencegah infiltrasi oleh agen musuh. Ini mencakup pengawasan terhadap individu dan kelompok yang berpotensi membahayakan keamanan nasional (Riehle, 2015). Kontra intelijen juga mempunyai fungsi respons terhadap ancaman hibrida. Dalam konteks konflik hibrida, kontraintelijen mencakup respons terhadap kombinasi ancaman dari aktor negara dan non-negara. Ini menuntut penyesuaian strategi intelijen dan kontraintelijen untuk menghadapi kompleksitas ancaman yang terus berkembang (Davies, 2024).

Dari pendapat lainnya, kontraintelijen yang didefinisikan oleh Wettering (2000), memiliki tiga fungsi utama, yaitu melindungi rahasia, yang mencakup pengamanan informasi yang dianggap penting untuk keamanan nasional, termasuk informasi militer, diplomatik, dan intelijen. Fungsi

berikutnya adalah menghalangi upaya spionase, yaitu kontraintelijen berusaha untuk mengidentifikasi dan mencegah upaya spionase yang dilakukan oleh negara atau kelompok asing. Selanjutnya fungsi kontraintelijen adalah menangkap mata-mata, artinya salah satu tugas penting kontraintelijen adalah menangkap individu yang berusaha mengkhianati negara dengan memberikan informasi kepada pihak asing.

Strategi kontraintelijen dapat dibagi menjadi dua kategori utama: defensif dan ofensif. Kontraintelijen Strategi defensif adalah strategi yang fokus pada perlindungan informasi sensitif dan mencegah infiltrasi musuh. Ciri dari strategi ini adalah melibatkan prosedur keamanan rutin, seperti pemeriksaan latar belakang dan pengawasan komunikasi. Contoh: Upaya untuk melindungi data sensitif di lembaga pemerintah dari akses yang tidak sah. Strategi berikutnya adalah ofensif yaitu strategi yang bertujuan untuk mengganggu dan melemahkan operasi intelijen musuh. Ciri dari strategi ini adalah melibatkan infiltrasi pada jaringan musuh, pengumpulan informasi, dan operasi penipuan. Contoh: Operasi yang dilakukan oleh CIA untuk mengidentifikasi dan menangkap agen-agen KGB selama Perang Dingin (Prunckun, 2019).

### **Komponen dan Urgensi Kontraintelijen**

Kontraintelijen merupakan salah satu aspek krusial dalam menjaga keamanan informasi dan melindungi kepentingan suatu negara atau organisasi. Dalam konteks ini, Prunckun (2019) mengidentifikasi beberapa komponen penting yang membentuk kerangka kerja kontraintelijen. Komponen-komponen ini tidak hanya berfungsi untuk melindungi informasi sensitif, tetapi juga untuk mengantisipasi dan merespons berbagai

ancaman yang mungkin muncul dari pihak musuh. Dengan memahami dan menerapkan prinsip-prinsip ini, suatu entitas dapat memperkuat pertahanan mereka terhadap potensi pelanggaran dan intrusi. Kontraintelijen mempunyai beberapa komponen, terutama yang dijabarkan oleh Prunckun (2019), sebagai berikut:

*Pertama, deterrence (Pencegahan):* Pencegahan adalah kemampuan untuk mencegah musuh dari mengakses informasi sensitif. Ini melibatkan pengembangan ancaman yang dapat membuat musuh berpikir dua kali sebelum mencoba melakukan penetrasi (Prunckun, 2019).

*Kedua, detection (Deteksi):* Deteksi adalah tindakan untuk mengetahui bahwa suatu peristiwa telah terjadi yang berhubungan dengan pelanggaran atau potensi pelanggaran informasi rahasia. Ini mencakup identifikasi individu yang terlibat dan pengumpulan fakta yang menunjukkan bahwa pelanggaran telah terjadi (Prunckun, 2019).

*Ketiga, deception (Penipuan):* Penipuan melibatkan upaya untuk menyesatkan pengambil keputusan musuh tentang operasi, kemampuan, atau niat lembaga. Tujuannya adalah untuk membuat musuh bertindak dengan cara yang tidak efektif (Prunckun, 2019).

*Keempat, neutralization (Netralisasi):* Netralisasi adalah tindakan untuk menghalangi operasi pengumpulan informasi musuh. Ini dapat dilakukan melalui penghancuran atau penundaan operasi musuh, sehingga mereka tidak dapat mencapai tujuan mereka (Prunckun, 2019).

*Keempat, counter espionage (Kontraespionase):* Ini adalah aspek ofensif dari kontraintelijen yang berfokus pada pengumpulan informasi dari layanan intelijen

musuh dan mengganggu operasi mereka (Prunckun, 2019).

*Kelima, security Measures (Langkah Keamanan):* Ini mencakup berbagai tindakan fisik dan prosedural yang dirancang untuk melindungi informasi sensitif dan mencegah akses tidak sah (Prunckun, 2019).

Secara keseluruhan, komponen-komponen kontraintelijen yang dijabarkan oleh Prunckun (2019) memberikan gambaran yang jelas tentang strategi yang diperlukan untuk melindungi informasi sensitif dari ancaman eksternal. Dari pencegahan hingga netralisasi, setiap elemen memiliki peran penting dalam menciptakan sistem pertahanan yang efektif. Dengan mengintegrasikan langkah-langkah keamanan yang tepat dan menerapkan teknik-teknik deteksi serta penipuan, organisasi dapat meningkatkan kemampuan mereka dalam menghadapi tantangan yang kompleks di era informasi saat ini. Melalui pemahaman yang mendalam tentang kontraintelijen, kita dapat lebih siap untuk melindungi aset-aset berharga dari ancaman yang terus berkembang.

Kontraintelijen memiliki urgensi yang sangat tinggi dalam konteks keamanan nasional, militer, dan bisnis. Dalam dunia yang semakin kompleks dan terhubung, ancaman terhadap informasi sensitif dan operasi rahasia semakin meningkat. Kontraintelijen berfungsi sebagai garis pertahanan pertama yang melindungi lembaga dari infiltrasi dan pengumpulan informasi oleh musuh (Prunckun, 2019). Tanpa adanya kontraintelijen yang efektif, lembaga akan rentan terhadap serangan yang dapat mengakibatkan kebocoran informasi, kerugian finansial, dan bahkan ancaman terhadap keselamatan individu. Urgensi dari kontraintelijen adalah sebagai berikut:

*Pertama, perlindungan Informasi Sensitif:* Kontraintelijen berperan penting

dalam menjaga kerahasiaan informasi yang vital bagi operasi lembaga. Ini mencakup data yang berkaitan dengan keamanan nasional, strategi militer, dan informasi bisnis yang bersifat kompetitif (Prunckun, 2019).

*Kedua, deteksi Ancaman:* Dengan adanya sistem kontraintelijen, lembaga dapat lebih cepat mendeteksi upaya penetrasi oleh musuh, sehingga dapat mengambil tindakan pencegahan yang diperlukan sebelum kerusakan terjadi (Prunckun, 2019).

Urgensi kontraintelijen sangat tinggi dalam konteks keamanan nasional, militer, dan bisnis, terutama di dunia yang semakin kompleks dan terhubung. Pertama, kontraintelijen berfungsi sebagai garis pertahanan pertama yang melindungi lembaga dari infiltrasi dan pengumpulan informasi oleh musuh, sehingga menjaga kerahasiaan informasi sensitif yang vital bagi operasi lembaga. Ini mencakup data terkait keamanan nasional, strategi militer, dan informasi bisnis yang bersifat kompetitif. Kedua, sistem kontraintelijen yang efektif memungkinkan lembaga untuk mendeteksi ancamannya dengan lebih cepat, sehingga tindakan pencegahan dapat diambil sebelum kerusakan terjadi. Tanpa adanya kontraintelijen yang handal, lembaga akan rentan terhadap serangan yang dapat mengakibatkan kebocoran informasi, kerugian finansial, dan ancaman terhadap keselamatan individu.

## **Kerangka Kerja Intelijen dan Kontraintelijen**

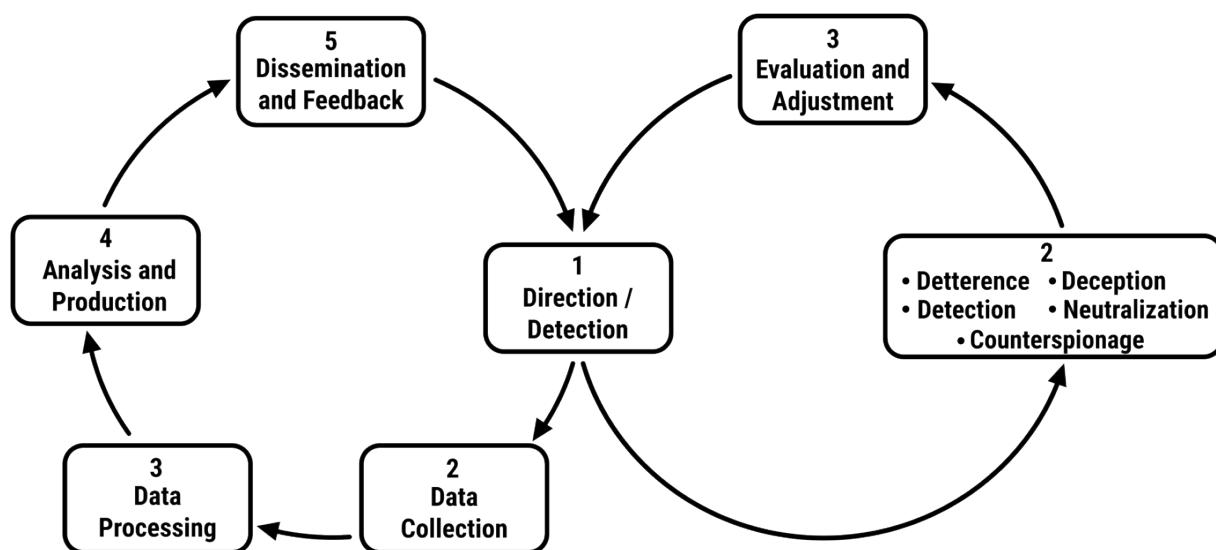
Dalam konteks kerangka kerja intelijen dan kontraintelijen, penting untuk memahami peran masing-masing dalam menjaga keamanan suatu negara. Intelijen berfungsi sebagai pengumpul, pengolah, dan penyebar informasi yang berkaitan dengan ancaman

potensial, baik dari luar maupun dalam negeri. Tujuannya adalah untuk memberikan wawasan yang diperlukan bagi pengambilan keputusan strategis. Intelijen juga berperan dalam misi penyelidikan dan analisis risiko, serta bekerja sama dengan berbagai lembaga terkait untuk memastikan informasi yang diperoleh akurat dan relevan.

Di sisi lain, kontraintelijen bertugas melindungi negara dari upaya penetrasi, spionase, dan sabotase oleh pihak-pihak yang ingin merugikan. Ini meliputi identifikasi dan penanggulangan aktivitas yang mencurigakan serta melindungi aset-aset vital, termasuk informasi sensitif. Kontraintelijen berfokus pada tindakan pencegahan dan mitigasi ancaman yang mungkin timbul dari kegiatan intelijen musuh.

Secara keseluruhan, kedua fungsi ini saling melengkapi dalam upaya menjaga stabilitas keamanan nasional. Kerjasama yang erat antara intelijen dan kontraintelijen sangat penting untuk mengidentifikasi ancaman yang kompleks dan berubah-ubah serta menyediakan respons yang efektif terhadap potensi risiko. Keduanya mengharuskan analisis yang mendalam, pengawasan yang ketat, dan adaptasi yang cepat dalam menghadapi dinamika ancaman yang terus berkembang.

Diagram kerangka kerja intelijen dan kontraintelijen ini menggambarkan berbagai langkah dan elemen penting dalam upaya melindungi informasi serta mencegah infiltrasi atau kegiatan intelijen yang merugikan. Terdapat beberapa tahapan vital, seperti pengumpulan intelijen, analisis ancaman, dan penerapan langkah-langkah keamanan. Dalam prosesnya, berbagai teknik pengawasan dan pengendalian digunakan untuk mengenali potensi risiko yang mungkin dihadapi, baik



Gambar 1: Diagram Kerangka Kerja Intelijen dan Kontraintelijen Sumber: diolah oleh peneliti

dari dalam maupun luar organisasi. Diagram ini juga menekankan pentingnya koordinasi antarunit untuk meningkatkan efektivitas pertahanan dan respon terhadap segala bentuk ancaman yang ada.

### Manfaat Kontraintelijen

Kontraintelijen memainkan peran yang sangat penting dalam menjaga keamanan dan integritas informasi, baik di sektor pemerintah maupun swasta. Dengan berbagai manfaat yang ditawarkannya, kontraintelijen tidak hanya berfungsi sebagai alat perlindungan, tetapi juga sebagai pendorong bagi pengambilan keputusan yang lebih baik dan lebih strategis. Prunckun (2019) mengidentifikasi sejumlah manfaat utama dari kontraintelijen, yang mencakup peningkatan keamanan, pencegahan kerugian finansial, dan peningkatan kepercayaan publik. Dalam dunia yang semakin kompleks dan terhubung, pemahaman tentang manfaat ini menjadi semakin relevan. Berikut adalah beberapa manfaat utama:

*Pertama*, meningkatkan Keamanan: Kontraintelijen membantu meningkatkan keamanan dengan menerapkan langkah-

langkah pencegahan dan deteksi yang efektif. Ini menciptakan lingkungan yang lebih aman bagi operasi lembaga (Prunckun, 2019).

*Kedua*, mendukung Pengambilan Keputusan: Dengan informasi yang terlindungi dan analisis yang tepat, kontraintelijen memberikan dukungan yang diperlukan untuk pengambilan keputusan yang lebih baik. Ini memungkinkan pemimpin untuk merumuskan kebijakan yang lebih efektif dan responsif terhadap ancaman yang ada (Prunckun, 2019).

*Ketiga*, mencegah Kerugian Finansial dan Reputasi: Dengan melindungi informasi sensitif, kontraintelijen membantu mencegah kerugian finansial yang dapat timbul akibat kebocoran data atau serangan siber. Selain itu, menjaga reputasi lembaga juga menjadi salah satu manfaat penting dari kontraintelijen (Prunckun, 2019).

*Keempat*, meningkatkan Kepercayaan Publik: Ketika lembaga dapat menunjukkan bahwa mereka memiliki sistem kontraintelijen yang efektif, hal ini dapat meningkatkan kepercayaan publik terhadap kemampuan mereka dalam melindungi informasi dan menjaga keamanan (Prunckun, 2019).

Secara keseluruhan, manfaat kontraintelijen yang luas menunjukkan betapa pentingnya pendekatan proaktif dalam melindungi informasi sensitif dan menjaga keamanan lembaga. Dengan menerapkan langkah-langkah pencegahan dan deteksi yang efektif, serta mendukung pengambilan keputusan yang tepat, kontraintelijen tidak hanya melindungi aset-aset berharga, tetapi juga berkontribusi pada reputasi dan kepercayaan publik. Dalam menghadapi ancaman yang terus berkembang, investasi dalam sistem kontraintelijen yang solid menjadi suatu keharusan bagi setiap organisasi yang ingin bertahan dan berkembang di era informasi ini.

### Konsep Operasi Kontraintelijen

Operasi kontraintelijen merupakan bagian integral dari strategi keamanan nasional yang bertujuan untuk melindungi negara dari ancaman yang berasal dari intelijen musuh, spionase, dan aktivitas subversif lainnya. Dalam konteks ini, kontraintelijen tidak hanya berfungsi untuk mendeteksi dan mencegah ancaman, tetapi juga untuk melindungi informasi sensitif dan menjaga integritas lembaga negara.

Menurut Lowenthal (2017), tujuan utama dari operasi kontraintelijen adalah untuk mengidentifikasi, mencegah, dan mengatasi kegiatan intelijen yang merugikan, serta untuk melindungi sumber daya dan informasi yang vital bagi keamanan nasional.

Operasi kontraintelijen melibatkan berbagai metode yang dirancang untuk melindungi kepentingan nasional dari ancaman intelijen musuh. Salah satu pendekatan yang digunakan adalah pencegahan, di mana tindakan diambil untuk mencegah kegiatan intelijen musuh sebelum mereka dapat

dilaksanakan. Ini termasuk pengawasan terhadap individu atau kelompok yang dicurigai terlibat dalam aktivitas spionase (Bamford, 2012). Selain itu, deteksi menjadi proses penting dalam operasi kontraintelijen, yang melibatkan identifikasi dan pengumpulan informasi mengenai kegiatan intelijen musuh. Deteksi dapat dilakukan melalui berbagai metode, termasuk pengawasan fisik dan elektronik, seperti penggunaan kamera, penyadapan telepon, dan analisis data (Hoffman, 2006; Lyon, 2003).

Metode lain yang krusial adalah penggagalan, di mana tindakan diambil untuk menggagalkan operasi intelijen musuh yang sedang berlangsung. Ini bisa melibatkan penangkapan agen musuh atau penghancuran jaringan spionase yang ada (Richelson, 2016). Selain itu, rekrutmen dan penanaman informan menjadi strategi yang efektif, di mana individu dengan akses ke informasi sensitif digunakan untuk memberikan intelijen yang berguna bagi negara. Proses ini sering kali melibatkan teknik manipulasi dan persuasi (Friedman, 2014).

Infiltrasi juga merupakan metode yang digunakan, di mana agen kontraintelijen ditempatkan dalam organisasi atau kelompok yang dicurigai untuk mengumpulkan informasi dari dalam (Bamford, 2012). Terakhir, operasi psikologis memanfaatkan propaganda dan disinformasi untuk mempengaruhi persepsi publik serta mengganggu operasi musuh (Richelson, 2016). Dengan menggabungkan berbagai metode ini, operasi kontraintelijen dapat lebih efektif dalam melindungi negara dari ancaman yang kompleks.

Dari pandangan lain, Harry Rositzke menjelaskan bahwa operasi kontraintelijen melibatkan berbagai metode yang dirancang untuk mengidentifikasi dan mengatasi ancaman

dari musuh. Salah satu pendekatan utama adalah pengawasan dan penetrasi, di mana agen kontraintelijen mengawasi aktivitas agen musuh dan berusaha mengidentifikasi jaringan mereka. Ini mencakup pemantauan pertemuan antara agen musuh dan informan lokal, yang dapat memberikan wawasan berharga tentang rencana dan strategi musuh. Selain itu, penggunaan agen ganda menjadi strategi penting, di mana individu yang telah direkrut oleh musuh dimanfaatkan untuk memberikan informasi yang menyesatkan atau untuk mengungkap operasi yang sedang dilakukan oleh pihak lawan (Rositzke, 1988).

Metode lain yang juga ditekankan oleh Rositzke adalah penyelidikan dan interogasi, di mana agen kontraintelijen melakukan interogasi terhadap individu yang dicurigai terlibat dalam kegiatan intelijen musuh. Proses ini bertujuan untuk mendapatkan informasi lebih lanjut yang dapat membantu dalam merumuskan strategi kontraintelijen yang lebih efektif. Dengan menggabungkan berbagai metode ini, operasi kontraintelijen dapat lebih efektif dalam mengidentifikasi dan mengatasi ancaman, serta melindungi kepentingan nasional dari infiltrasi dan spionase yang dilakukan oleh musuh (Rositzke, 1988).

## **Operasi Kontraintelijen di Berbagai Negara**

Berbagai negara telah melaksanakan operasi kontraintelijen yang signifikan sepanjang sejarah untuk melindungi kepentingan nasional mereka dari ancaman intelijen musuh. Di Amerika Serikat, Central Intelligence Agency (CIA) meluncurkan Operasi Chaos selama Perang Vietnam, sebuah program kontraintelijen yang bertujuan untuk memantau dan mengganggu gerakan anti-perang di dalam negeri. Operasi ini melibatkan

pengumpulan informasi tentang individu dan kelompok yang terlibat dalam protes, serta upaya untuk memanipulasi opini publik (Prunckun, 2019).

Sementara itu, Inggris menunjukkan kecanggihan dalam taktik penipuan melalui Operasi TIGRESS pada tahun 1952. Operasi ini dirancang untuk mengelabui Uni Soviet mengenai waktu dan lokasi uji coba bom atom pertama Inggris, sekaligus melindungi informasi sensitif dari pengintaian (Dylan, 2015). Di sisi lain, Rusia, melalui Komite Keamanan Negara (KGB), melakukan berbagai operasi kontraintelijen di negara-negara Barat selama Perang Dingin. Operasi ini mencakup infiltrasi ke dalam organisasi politik dan sosial untuk mengumpulkan informasi dan memengaruhi kebijakan, dengan contoh perekrutan agen di kalangan diplomat dan akademisi (Andrew, 2009).

Israel juga memiliki sejarah panjang dalam operasi kontraintelijen yang agresif. Setelah serangan teroris di Olimpiade Munich pada tahun 1972, Israel meluncurkan Operasi Wrath of God untuk memburu dan membunuh anggota kelompok teroris yang bertanggung jawab. Operasi ini melibatkan intelijen yang mendalam dan taktik kontraintelijen untuk menghindari deteksi (Black, 2005).

Di Asia Selatan, India melaksanakan operasi kontraintelijen selama konflik Kargil pada tahun 1999. Operasi ini bertujuan untuk mengidentifikasi dan mengusir pasukan Pakistan yang menyusup ke wilayahnya, melibatkan pengumpulan intelijen melalui pengintaian dan pengawasan (Gupta, 2000). Tetangganya, Pakistan, juga mengandalkan kontraintelijen dalam Operasi Zarb-e-Azb, sebuah operasi militer yang diluncurkan oleh Angkatan Bersenjata Pakistan untuk melawan terorisme di wilayah Waziristan Utara. Dalam

operasi ini, kontraintelijen berperan penting dalam mengidentifikasi dan menargetkan kelompok teroris (Khan, 2015).

China meluncurkan Operasi Fox Hunt, sebuah program kontraintelijen yang dirancang untuk menangkap para pembangkang dan koruptor yang mlarikan diri ke luar negeri. Operasi ini melibatkan pengumpulan intelijen dan taktik infiltrasi untuk mengembalikan individu-individu tersebut ke China (Shambaugh, 2013).

Di Eropa, Prancis melakukan Operasi Cobalt untuk mengawasi dan mengganggu aktivitas kelompok separatis di Aljazair, melibatkan pengumpulan intelijen dan penggunaan taktik penipuan untuk mengelabui musuh (Rojas, 2015). Sementara itu, Jerman (Barat) bersama NATO melaksanakan Operasi Gladio selama Perang Dingin untuk melawan ancaman komunis, yang melibatkan pembentukan jaringan rahasia yang siap bertindak jika terjadi invasi Soviet (De Jong, 2006).

Di Afrika, Kongres Nasional Afrika (ANC) melaksanakan Operasi Vula untuk mengirimkan anggotanya ke dalam Afrika Selatan selama apartheid. Operasi ini melibatkan pengumpulan intelijen dan penyusupan ke dalam struktur pemerintah (Hough, 2002).

Selain oleh negara, kontraintelijen juga dilakukan oleh *non-state-actor*. Salah satu contoh paling mencolok dari penggunaan kontraintelijen oleh *non-state-actor* dalam konteks terorisme adalah serangan 9/11 yang dilakukan oleh Al-Qaeda. Menurut Ilardi (2009), Al-Qaeda berhasil melaksanakan serangan tersebut berkat persiapan intelijen dan kontraintelijen yang matang. Mereka melakukan pengumpulan informasi yang mendalam tentang target dan lingkungan

operasional mereka, yang memungkinkan mereka untuk merencanakan serangan dengan sangat efektif.

Al-Qaeda melakukan aksi intelijen dengan mengumpulkan informasi tentang keamanan bandara, pola perjalanan, dan prosedur penerbangan. Mereka menggunakan teknik pengintaian untuk memahami bagaimana dan kapan mereka dapat menyerang tanpa terdeteksi. Al-Qaeda juga menerapkan taktik kontraintelijen untuk melindungi operasi mereka dari pengawasan.

Mereka menggunakan komunikasi yang aman dan menghindari pola yang mencurigakan. Keberhasilan serangan ini menunjukkan pentingnya intelijen dalam merencanakan dan melaksanakan operasi teroris.

### Tantangan dalam Kontraintelijen

Kontraintelijen memainkan peran yang sangat penting dalam menjaga keamanan nasional dan melindungi informasi sensitif dari ancaman eksternal. Namun, pelaksanaan fungsi ini tidaklah tanpa tantangan. Berbagai isu etika dan hukum muncul, terutama yang berkaitan dengan privasi individu dan hak asasi manusia. Agen kontraintelijen sering kali dihadapkan pada dilema etis yang memerlukan pertimbangan matang, di mana keputusan yang diambil dapat memiliki dampak luas. Dengan memahami tantangan yang dihadapi dalam operasi kontraintelijen, diharapkan pembaca dapat menghargai kompleksitas dan pentingnya peran kontraintelijen dalam melindungi negara dari berbagai ancaman yang terus berkembang (Prunckun, 2019). Beberapa tantangan tersebut meliputi:

*Pertama*, perkembangan Teknologi: Dengan kemajuan teknologi, metode spionase menjadi semakin canggih. Penggunaan

perangkat lunak dan perangkat keras yang dapat menyusup ke sistem informasi menjadi tantangan besar bagi kontraintelijen (Wettering, 2000).

*Kedua*, keterbatasan Sumber Daya: Banyak lembaga kontraintelijen menghadapi keterbatasan dalam hal anggaran dan sumber daya manusia. Hal ini dapat menghambat kemampuan mereka untuk melakukan pengawasan dan investigasi yang efektif (Lyman, 2023).

*Ketiga*, isu Etika dan Hukum: Keseimbangan antara Keamanan Nasional, Etika, dan Hak Asasi Manusia Kegiatan kontraintelijen sering kali berada di batasan antara keamanan nasional dan hak asasi manusia, menimbulkan dilema etis yang kompleks. Tindakan seperti pengawasan massal, infiltrasi, dan penggunaan informan, meskipun dianggap perlu untuk melindungi negara, berpotensi melanggar privasi individu dan hak-hak sipil (Lyon, 2003; Zedner, 2009). Misalnya, pengumpulan data komunikasi secara besar- besaran dapat mengikis kebebasan sipil, sementara teknik interogasi yang tidak manusiawi, meskipun dilarang oleh hukum internasional, masih menjadi perhatian dalam beberapa konteks (United Nations, 2011; Walzer, 2015). Oleh karena itu, penting untuk mengembangkan kerangka etika yang jelas yang mencakup tanggung jawab moral, transparansi, dan akuntabilitas. Mekanisme pengawasan yang kuat dari parlemen, badan independen, dan peradilan sangat krusial untuk mencegah penyalahgunaan kekuasaan dan menjaga kepercayaan publik (Haggerty & Ericson, 2000).

*Keempat*, era Digital, Disinformasi, dan Perang Kognitif (Media baru), khususnya penggunaan media sosial dan platform digital, telah menjadi tantangan besar dalam

penggunaan data dan komunikasi. Fenomena disinformasi dan misinformasi memiliki peran penting dalam melakukan ekstraksi data dan informasi, serta memanipulasi persepsi publik (ACSS, 2024; Better World Campaign, 2024). Kontraintelijen kini harus menghadapi “perang kognitif” (cognitive warfare), di mana aktor negara dan non-negara secara sistematis menyebarkan narasi palsu dan propaganda untuk memengaruhi keyakinan, emosi, dan perilaku target populasi, serta merusak kohesi sosial dan kepercayaan terhadap institusi pemerintah (Putter, 2024). Tantangan ini menuntut adaptasi kontraintelijen melalui pemanfaatan analisis data besar dan kecerdasan buatan untuk mendeteksi pola penyebaran disinformasi, serta pengembangan strategi kontra-narasi yang efektif tanpa mengorbankan prinsip-prinsip demokrasi dan kebebasan informasi.

Menghadapi kompleksitas tantangan ini, keberhasilan kontraintelijen di era modern tidak hanya bergantung pada kecanggihan teknologi atau besarnya sumber daya, melainkan juga pada kemampuan adaptasi yang berkelanjutan dan komitmen teguh terhadap prinsip-prinsip etika dan hukum. Keseimbangan antara efektivitas operasional dan penghormatan terhadap hak asasi manusia menjadi krusial untuk menjaga legitimasi dan kepercayaan publik. Dengan demikian, kontraintelijen harus terus berinovasi dalam strategi dan taktiknya, sembari memperkuat kerangka pengawasan dan akuntabilitas, demi melindungi keamanan nasional dari ancaman yang terus berevolusi di tengah lanskap informasi yang semakin rumit.

#### **Etika dalam Kontraintelijen**

Kontraintelijen berfungsi untuk mendeteksi, mencegah, dan merespons

ancaman terhadap keamanan nasional. Namun, dalam menjalankan tugas ini, agen kontraintelijen sering kali dihadapkan pada dilema etis. Misalnya, penggunaan teknik penyadapan atau infiltrasi dapat melanggar privasi individu, sementara pengumpulan informasi dapat melibatkan manipulasi atau penipuan. Oleh karena itu, penting untuk mengembangkan kerangka etika yang jelas untuk membimbing tindakan kontraintelijen. Beberapa aspek etika dalam kontraintelijen adalah sebagai berikut:

*Pertama*, tanggung Jawab Moral: agen kontraintelijen memiliki tanggung jawab moral untuk melindungi negara dan warganya. Namun, tanggung jawab ini harus seimbang dengan penghormatan terhadap hak asasi manusia. Menurut Walzer (2015), tindakan yang diambil dalam nama keamanan harus selalu mempertimbangkan dampaknya terhadap individu dan masyarakat. Misalnya, penahanan tanpa proses hukum dapat dianggap sebagai pelanggaran hak asasi manusia, meskipun mungkin dianggap perlu untuk keamanan nasional.

*Kedua*, transparansi dan Akuntabilitas: transparansi adalah elemen kunci dalam etika kontraintelijen. Masyarakat berhak mengetahui bagaimana informasi dikumpulkan dan digunakan. Menurut Haggerty dan Ericson (2000), kurangnya transparansi dapat mengarah pada penyalahgunaan kekuasaan dan hilangnya kepercayaan publik. Oleh karena itu, penting bagi lembaga kontraintelijen untuk memiliki mekanisme akuntabilitas yang jelas, termasuk pengawasan oleh badan independen.

*Ketiga*, perlindungan Hak Asasi Manusia: perlindungan hak asasi manusia harus menjadi prioritas dalam operasi kontraintelijen. Menurut United Nations (2011), semua

tindakan yang diambil oleh negara harus mematuhi hukum internasional dan standar hak asasi manusia. Ini termasuk perlindungan terhadap individu yang mungkin menjadi sasaran operasi kontraintelijen. Misalnya, penggunaan teknik penyiksaan atau perlakuan tidak manusiawi dalam interrogasi harus dilarang secara tegas.

Pengumpulan informasi sering kali melibatkan dilema etis. Teknik seperti penyadapan telepon atau pengintaian dapat dianggap perlu untuk mencegah ancaman, tetapi juga dapat melanggar privasi individu. Menurut Lyon (2003), penting untuk mengevaluasi apakah manfaat dari pengumpulan informasi tersebut sebanding dengan risiko pelanggaran privasi. Oleh karena itu, lembaga kontraintelijen harus mengembangkan pedoman yang jelas mengenai teknik yang dapat digunakan.

Salah satu tantangan utama dalam kontraintelijen adalah menemukan keseimbangan antara keamanan dan kebebasan individu. Menurut Zedner (2009), tindakan yang diambil untuk meningkatkan keamanan tidak boleh mengorbankan kebebasan sipil. Oleh karena itu, penting untuk memiliki batasan yang jelas mengenai tindakan yang dapat diambil oleh agen kontraintelijen.

Etika dalam kontraintelijen adalah aspek yang sangat penting dan kompleks. Agen kontraintelijen harus selalu mempertimbangkan tanggung jawab moral, transparansi, dan perlindungan hak asasi manusia dalam menjalankan tugas mereka. Dengan mengembangkan kerangka etika yang jelas, lembaga kontraintelijen dapat memastikan bahwa tindakan mereka tidak hanya efektif dalam melindungi negara, tetapi juga menghormati nilai-nilai dasar kemanusiaan.

## **Ancaman Intelijen Asing terhadap IKN dan Manfaat Kontraintelijen**

Mengingat posisi strategis Ibu Kota Nusantara (IKN) sebagai pusat pemerintahan dan simbol ketahanan nasional, kontraintelijen memegang peran krusial dalam menghadapi spektrum ancaman intelijen asing yang telah diidentifikasi sebelumnya. Penerapan kontraintelijen di IKN tidak hanya berorientasi pada pertahanan pasif, melainkan sebagai elemen proaktif yang esensial untuk memastikan keamanan, keberlanjutan pembangunan, dan ketahanan IKN dari segala bentuk intervensi dan eksploitasi yang merugikan kepentingan nasional. Manfaat kontraintelijen dalam melindungi IKN mencakup peningkatan keamanan secara keseluruhan dan dukungan terhadap pengambilan keputusan strategis.

Dengan menerapkan langkah-langkah pencegahan dan deteksi yang efektif, kontraintelijen menciptakan lingkungan yang lebih aman bagi operasi pemerintah dan aset-aset vital di IKN. Informasi yang terlindungi dan analisis yang tepat dari kontraintelijen memungkinkan para pemimpin untuk merumuskan kebijakan yang lebih efektif dan responsif terhadap ancaman yang ada, baik yang bersifat tradisional maupun hibrida (Reed & Mc Ivor, 2005). Selain itu, kontraintelijen juga berperan dalam mencegah kerugian finansial dan menjaga reputasi lembaga, yang sangat penting bagi keberlanjutan pembangunan IKN. Kepercayaan publik terhadap kemampuan pemerintah dalam melindungi informasi dan menjaga keamanan juga akan meningkat seiring dengan efektivitas sistem kontraintelijen yang diterapkan (Riehle, 2015).

## **SIMPULAN**

Kontraintelijen terbukti menjadi elemen integral dan dinamis dalam strategi ketahanan

nasional, esensial untuk melindungi negara dari spektrum ancaman intelijen asing yang terus berevolusi. Adaptasi berkelanjutan, dari praktik kuno hingga menghadapi ancaman hibrida kontemporer seperti serangan siber dan perang kognitif, merupakan prasyarat mutlak bagi keberhasilan kontraintelijen. Fungsi-fungsi utamanya, yang mencakup pencegahan, deteksi, penipuan, netralisasi, kontraespionase, dan langkah keamanan, secara kolektif berkontribusi pada peningkatan keamanan nasional, dukungan pengambilan keputusan strategis, pencegahan kerugian finansial dan reputasi, serta pembangunan kepercayaan publik.

Secara khusus, bagi Ibu Kota Nusantara (IKN) sebagai proyek strategis nasional dan simbol ketahanan Indonesia, peran kontraintelijen menjadi sangat sentral. Keberhasilan IKN sebagai kota cerdas dan berkelanjutan sangat bergantung pada efektivitas sistem kontraintelijen yang proaktif dalam melindungi aset strategis, infrastruktur vital, dan informasi pemerintah yang sensitif dari spionase, sabotase, subversi, dan disinformasi. Ini menuntut integrasi perlindungan infrastruktur digital dan fisik, pengamanan data, serta pencegahan infiltrasi dan disinformasi sebagai prioritas utama dalam setiap aspek perencanaan dan operasional IKN.

Namun, pelaksanaan operasi kontraintelijen tidaklah tanpa tantangan signifikan. Perkembangan teknologi informasi yang pesat, keterbatasan sumber daya, dan isu etika-hukum yang kompleks—terutama dalam menyeimbangkan keamanan nasional dengan privasi individu dan hak asasi manusia—menuntut adaptasi berkelanjutan. Dalam menghadapi ancaman era digital seperti perang kognitif, kontraintelijen harus terus berinovasi,

termasuk melalui pemanfaatan analisis data besar dan kecerdasan buatan, untuk mendeteksi pola penyebaran disinformasi dan mengembangkan strategi kontra-narasi yang efektif.

Oleh karena itu, investasi berkelanjutan dalam kapabilitas kontraintelijen, diiringi dengan kerangka etika yang kuat, kolaborasi lintas sektor antar lembaga, transparansi, dan akuntabilitas, bukan hanya sebuah pilihan, melainkan sebuah keharusan mutlak. Dengan demikian, kontraintelijen dapat terus berinovasi dalam strategi dan taktiknya, sembari memperkuat kerangka pengawasan, demi melindungi keamanan nasional dan memastikan ketahanan bangsa yang adaptif serta tangguh di tengah dinamika global yang penuh ketidakpastian.

## DAFTAR PUSTAKA

- ACSS. (2024). *Mapping a surge of disinformation in Africa*. Africa Center for Strategic Studies. Retrieved from <https://africacenter.org/wp-content/uploads/2024/05/Regional- Map-of- Disinformation-in-Africa-2024.pdf>
- Aldrich, R. J. (2001). *The hidden hand*. John Murray.
- Andrew, C. (2009). *The defence of the realm: The authorized history of MI5*. Penguin.
- Ashley, C. (2004). *CIA spymaster*. Pelican Press.
- Bachmann, D., Putter, D., & Duczynski, G. (2023). Covert action as hybrid warfare—clarifying the semantics. *Journal of Information Warfare*, 22(3), 60–77.
- Bamford, J. (2012). *The shadow factory: The ultra-secret NSA from 9/11 to the eavesdropping on America*. Doubleday.
- Barnea, A. (2020). Filling the void in counterintelligence literature. *International Journal of Intelligence and CounterIntelligence*, 33(1), 199–202. <https://doi.org/10.1080/08850607.2019.1675487>
- Better World Campaign. (2024). *The damaging deluge of disinformation: What researchers are learning from Africa's digital boom*. Retrieved from <https://betterworldcampaign.org/blog/disinformation>
- Black, I. (2005). *Israel's secret wars: A history of Israel's intelligence services*. St. Martin's Press.
- Braman, S. (2006). *The information revolution: A historical perspective*. Routledge.
- Calista, D. J. (2014). Enduring inefficiencies in counterintelligence by reducing Type I and Type II errors through parallel systems: A principal-agent typology. *International Journal of Intelligence and CounterIntelligence*, 27(1), 109–131. <https://doi.org/10.1080/08850607.2014.842809>
- Cathcart, B. (1994). *Test of greatness: Britain's struggle for the atomic bomb*. John Murray.
- Daugherty, W. J. (2007). The role of covert action. In K. J. Loch (Ed.), *Handbook of intelligence studies* (Vol. 2, pp. 279–288). Routledge.
- Davies, P. H. J. (2024). Counterintelligence and escalation from hybrid to total war in the Russo-Ukrainian conflict 2014–2024. *Intelligence and National Security*, 39(3), 496–514. <https://doi.org/10.1080/02684527.2024.2329419>
- Davies, P. H. J., & Steward, T. J. (2024). The trouble with TESSOC: The coming crisis in British and allied military counterintelligence doctrine. *Defence Studies*.

- De Jong, L. (2006). *The secret war: Gladio and NATO's stay-behind armies*. Routledge.
- Dheeraj, P. C. (2018). Seaborne terrorism and counterintelligence in India: Challenges and concerns. *Journal of the Indian Ocean Region*, 14(3), 277–295. <https://doi.org/10.1080/19480881.2018.1519054>
- Dylan, H. (2015). Operation TIGRESS: Deception for counterintelligence and Britain's 1952 atomic test. *Journal of Intelligence History*, 14(1), 1–15. <https://doi.org/10.1080/16161262.2014.943996>
- Goodman, M. (2007). *Spying on the nuclear bear*. Stanford University Press.
- Gupta, A. (2000). *Kargil: The saga of valor*. HarperCollins.
- Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology*, 51(4), 605–622.
- Hennessy, P. (2000). *The prime minister: The office and its holders since 1945*. Penguin.
- Hoffman, B. (2006). *Inside terrorism*. Columbia University Press.
- Hosaka, S. (2025). The Sino–Soviet intelligence war: The KGB counterintelligence perspective. *International Journal of Intelligence and CounterIntelligence*, 38(2), 462–494. <https://doi.org/10.1080/08850607.2024.2350423>
- Hough, M. (2002). *The ANC and the struggle for a new South Africa*. Zed Books.
- Ilardi, G. J. (2009). The 9/11 attacks—A study of Al Qaeda's use of intelligence and counterintelligence. *Studies in Conflict & Terrorism*, 32(3), 171–187. <https://doi.org/10.1080/10576100802670803>
- Ingesson, T., & Andersson, M. (2024). Clandestine communications in cyber-denied environments. *Journal of Policing, Intelligence and Counter* *Terrorism*, 19(2), 144–165. <https://doi.org/10.1080/18335330.2023.2209578>
- Kent, S. (1949). *Strategic intelligence for American world policy*. Princeton University Press.
- Khan, A. (2015). *The war on terror: Pakistan's role and challenges*. Institute of Strategic Studies.
- Libicki, M. C. (1995). *What is information warfare?* National Defence University, Centre for Advanced CommandConcepts and Technology. <https://smallwarsjournal.com/documents/libicki.pdf>
- Lowenthal, M. M. (2017). *Intelligence: From secrets to policy* (7th ed.). CQ Press.
- Lyman, B. J. (2023). In the eye of the Sphinx: US army intelligence collection and surveillance, 1965–1970. *Journal of Intelligence History*, 22(3), 376–397. <https://doi.org/10.1080/16161262.2022.2099190>
- Lyon, D. (2003). *Surveillance as social sorting: Privacy, risk, and digital discrimination*. Routledge.
- Magee, A. C. (2024). Counterintelligence black swan: KGB deception, countersurveillance, and active measures operation. *International Journal of Intelligence and CounterIntelligence*, 37(1), 232–264. <https://doi.org/10.1080/08850607.2023.2192374>
- Mahnken, T. G. (2007). *The limits of military innovation: The United States and the Soviet Union in the Cold War*. Routledge.
- Ndlovu-Gatsheni, S. J., & Ruhanya, P. (Eds.). (2020). *The history and political transition of Zimbabwe: From Mugabe to Mnangagwa*. Palgrave McMillan.
- Olson, J. M. (2019). *To catch a spy: The art of counterintelligence*. Georgetown University Press.

- Prados, J. (2006). *The family jewels: The CIA, secrecy, and presidential power*. The New Press.
- Prunckun, H. (2011). A grounded theory of counterintelligence. *American Intelligence Journal*, 29(2), 6–15. <https://doi.org/10.2307/26201945>
- Prunckun, H. (2019). *Counterintelligence theory and practice* (2nd ed.). Rowman & Littlefield.
- Putter, D. (2024). Navigating the interplay of cognitive warfare and counterintelligence in African security strategies: Insights and case studies. *Journal of Policing, Intelligence and Counter Terrorism*, 20(2), 173–192. <https://doi.org/10.1080/18335330.2024.2440873>
- Pyle, C. H. (1970, January). CONUS intelligence: The Army watches civilian politics. *Washington Monthly*.
- Reed, R. L. Jr., & Mc Ivor, A. D. (2005). Counterintelligence as a strategic asset: Thinking anew. *American Intelligence Journal*, 23(1), 64–66. <https://doi.org/10.2307/44327039>
- Richelson, J. T. (2007). *The U.S. intelligence community*. Westview Press.
- Riehle, K. P. (2015). A counterintelligence analysis typology. *American Intelligence Journal*, 32(1), 55–60. <https://doi.org/10.2307/26202104>
- Robarge, D. (2003). Moles, defectors, and deceptions: James Angleton and CIA counterintelligence. *Journal of Intelligence History*, 3(2), 21–49. <https://doi.org/10.1080/16161262.2003.10555085>
- Rojas, C. (2015). *The French secret services: From the Dreyfus Affair to the present*. Routledge.
- Rositzke, H. (1988). *The CIA's secret operations: Espionage, counterespionage, and covert action*. Westview Press.
- Selth, A. (2025). Spy versus spy: Myanmar's multiple counterintelligence challenges. *International Journal of Intelligence and CounterIntelligence*.
- Serscikov, G. (2024). Israel's intelligence services in Iran: Exploiting vulnerabilities for penetration. *International Journal of Intelligence and CounterIntelligence*, 37(1), 89– 120.
- Shaffer, R. (2022). Decoding the Samba spy scandal: False spies, counterintelligence and military intelligence in India. *Journal of Intelligence History*.
- Shambaugh, D. (2013). *China goes global: The partial power*. Oxford University Press.
- Smith, J. (2020). *Intelligence and warfare: The role of intelligence in World War II*. Historical Press.
- Stouder, M. D., & Gallagher, S. (2015). Counterintelligence outreach: Building a strategic capability. *International Journal of Intelligence and CounterIntelligence*.
- United Nations. (2011). *The United Nations and the protection of human rights*. United Nations.
- Van Cleve, M. K. (2007). *Counterintelligence and national strategy*. <https://apps.dtic.mil/sti/citations/ADA471485>
- Walzer, M. (2015). *Just and unjust wars: A moral argument with historical illustrations*. Basic Books.
- Wettering, F. L. (2000). Counterintelligence: The broken triad. *International Journal of Intelligence and Counter Intelligence*, 13 (3), 265–300. <https://doi.org/10.1080/08850600050140607>

- Yang, Z. (2022). The Chinese Communist Party's exploitation of the Second United Front: Intelligence and counterintelligence on a middle force territory. *Intelligence and National Security*, 37(1), 73–89. <https://doi.org/10.1080/02684527.2021.1984017>
- Zedner, L. (2009). Security, the state and the citizen: The changing face of security. *Theoretical Criminology*, 13(3), 299–318.
- Zegart, A. (2007). *Spying blind: The CIA, the FBI, and the origins of 9/11*. Princeton University Press.