

Perkembangan Militerisasi Teknologi:

Weaponization of Emerging Technologies

dan Dampaknya terhadap
HAM di Indonesia



**PERKEMBANGAN
MILITERISASI TEKNOLOGI
*WEAPONIZATION OF EMERGING
TECHNOLOGIES* DAN DAMPAKNYA
TERHADAP HAM DI INDONESIA**

Perkembangan Militerisasi Teknologi: *Weaponization of Emerging Technologies* dan Dampaknya terhadap HAM di Indonesia

Penulis

Adzkar Ahsinin

Ikhsan Yosarie

Nurul Izmi

Kezia Khatwani

Octania Wynn

Naira A. Wibisono

Editor

Sueb

Penata letak

Dodi Sanjaya

Ilustrator

Amry Al Mursaalat

Penerbit

Lembaga Studi dan Advokasi Masyarakat (ELSAM) 2026

Jl. Siaga II No. 31, Pejaten Barat, Pasar Minggu, Jakarta 12510



DAFTAR ISI

BAB I PENDAHULUAN	1
1. Latar Belakang	1
2. Rumusan Masalah	4
3. Metode Penelitian	5
BAB II TEKNOLOGI DWIGUNA, KOMPLEKS INDUSTRI-MILITER, DAN HAK ASASI MANUSIA	7
1. Teknologi Dwigunda	7
2. Kompleks Militer-Industri, Konteks Indonesia	17
3. Bagaimana Dampak HAM dalam Penggunaan Teknologi Surveillance oleh Militer?	25
4. Bagaimana Pengaturan dan Pertanggungjawaban Mengenai Militerisasi Teknologi?	49
5. Penggunaan Teknologi Dwiguna dalam Konteks Modernisasi Militer Indonesia dan Dampaknya Terhadap HAM	67
6. Teknologi Dwiguna dalam Konteks Kompleks Digital Industrial Militer: Demarkasi Sipil dan Militer yang Semakin Kabur	77
7. Irisan Kebangkitan Militerisasi dan Penggunaan Teknologi Dwi Guna: Identifikasi Dampaknya Terhadap HAM	118
BAB III	147
KESIMPULAN DAN REKOMENDASI	
Kesimpulan	147
Rekomendasi	148
DAFTAR PUSTAKA	149
PROFIL LEMBAGA	165

“Bahaya terbesar adalah ketakutan dalam kepala kita. Ketakutan yang disebarkan sistem yang ada kepada kita. Ketakutan inilah rintangan terbesar dalam perjuangan.”

Munir Said Thalib (1965-2004), Aktivis HAM

BAB I

PENDAHULUAN

1. Latar Belakang

Presiden Amerika Serikat Dwight D. Eisenhower pernah memperingatkan mengenai bahaya kompleks industri-militer (*military-industrial complex*) dalam pidato perpisahannya pada 17 Januari 1961. Peringatan tersebut disampaikan dalam konteks semakin eratnya keterkaitan antara institusi militer, industri persenjataan, dan pemerintahan. Eisenhower mengkhawatirkan pengaruh yang tidak semestinya dari kombinasi tersebut terhadap pengambilan keputusan pemerintah yang berpotensi membahayakan kebebasan dan proses demokratis.¹

Peringatan Eisenhower menjadi semakin relevan ketika perusahaan teknologi semakin terlibat dalam sektor pertahanan. Seiring dengan perkembangan teknologi, konfigurasi kompleks industri-militer tersebut mengalami perubahan. Jika sebelumnya industri persenjataan konvensional menjadi aktor utama dalam ekosistem pertahanan, perkembangan teknologi digital menghadirkan perusahaan *Big Tech* dengan kekuatan ekonomi dan teknologi yang semakin besar. Kekuatan tersebut bersumber dari penguasaan atas pengetahuan, penelitian dan pengembangan, serta infrastruktur digital dan teknologi mutakhir, seperti kecerdasan buatan dan komputasi awan, yang dibutuhkan baik dalam sektor sipil maupun militer. Keterlibatan *Big Tech* dalam sektor pertahanan tidak lagi terbatas pada penyediaan teknologi, tetapi juga mencerminkan pergeseran pusat kekuatan dalam kompleks industri-militer. Perubahan ini melahirkan fenomena yang dikenal sebagai kompleks industri-militer-digital (*digital-military-industrial complex*), yang ditandai oleh semakin besarnya peran dan pengaruh perusahaan teknologi dalam ekosistem pertahanan.²

Perubahan konfigurasi kompleks industri-militer tersebut juga berkaitan dengan perkembangan militerisasi teknologi (*militarisation of tech*), yang ditandai oleh semakin luasnya penggunaan teknologi untuk kepentingan militer. Tak hanya itu, militerisasi teknologi juga tercermin dari meluasnya pengaruh militer dalam ranah teknologi dan

¹ James Ledbetter, *Unwarranted Influence: Dwight D. Eisenhower and the Military-Industrial Complex* (New Haven, CT: Yale University Press, 2011).

² Andrea Coveri, Claudio Cozza, dan Dario Guarascio, "Big Tech and the US Digital-Military-Industrial Complex," *Intereconomics* 60, no. 2 (2025): 81–87, <https://doi.org/10.2478/ie-2025-0017>.

kehidupan sipil. Pengaruh tersebut dapat terwujud melalui keterlibatan aktor militer, perluasan peran dan praktik militer, serta penerapan cara pandang militer dalam pengembangan, pengadaan, dan penggunaan teknologi. Kecenderungan ini terlihat dalam empat fenomena berikut.³

Pertama, penggunaan sistem berbasis data untuk kepentingan militer. Teknologi pengawasan, analisis data, dan kecerdasan buatan semakin banyak digunakan dalam operasi militer, termasuk untuk memantau aktivitas, mengidentifikasi individu, dan menentukan sasaran. Di Israel, misalnya, militer menggunakan sistem kecerdasan buatan Lavender untuk menganalisis data pengawasan massal dan mengidentifikasi individu yang dicurigai sebagai anggota Hamas. Penggunaan sistem ini dilaporkan turut menyebabkan kesalahan identifikasi dan jatuhnya korban sipil.

Kedua, keterlibatan perusahaan teknologi dalam sektor pertahanan. Perusahaan *Big Tech* dan *startup* yang semula berfokus pada pengembangan teknologi dan infrastruktur untuk kebutuhan komersial dan sipil semakin memasuki sektor pertahanan. Keterlibatan ini antara lain terlihat dari penyediaan teknologi yang awalnya dikembangkan untuk pasar sipil, tetapi juga digunakan untuk kepentingan militer sebagai teknologi dwiguna (*dual-use technology*).

Ketiga, peralihan teknologi pertahanan ke sektor sipil. Teknologi yang digunakan dalam konflik semakin banyak dialihkan untuk penegakan hukum dan layanan publik. Salah satu contohnya adalah Palantir, yang menyediakan teknologi analisis data untuk kebutuhan militer, pengawasan migran, pemolisian prediktif, hingga layanan kesehatan.

Keempat, adaptasi teknologi konflik untuk kepentingan komersial. Teknologi yang digunakan dalam konflik juga diadaptasi untuk kepentingan komersial, seperti pemanfaatan teknologi pengenalan wajah yang digunakan dalam pengawasan di wilayah Palestina untuk keperluan di sektor sipil, seperti sekolah dan rumah sakit. Sebaliknya, teknologi komersial, seperti citra satelit, juga dimanfaatkan untuk kepentingan militer.

Keempat fenomena tersebut menunjukkan semakin kaburnya batas antara ranah militer dan sipil, baik dalam pengembangan dan penggunaan teknologi maupun dalam peran para aktor yang terlibat. Kekaburan ini menjadi persoalan ketika teknologi dan keterlibatan aktor militer meluas ke ranah sipil, sehingga memperluas praktik dan cara pandang militer dalam kehidupan masyarakat. Tanpa batasan hukum, transparansi, akuntabilitas, dan mekanisme pengawasan yang memadai, perkembangan tersebut

³ Privacy International, "What Is Militarisation of Tech?," <https://privacyinternational.org/long-read/5668/what-militarisation-tech>.

dapat meningkatkan risiko pelanggaran hak asasi manusia (HAM), termasuk hak atas privasi dan kebebasan berekspresi.

Dalam konteks Indonesia, keterlibatan perusahaan teknologi dalam sektor keamanan terlihat antara lain melalui kerja sama Huawei dan Badan Siber dan Sandi Negara (BSSN) di bidang keamanan siber. Sejak 2019, kedua pihak telah melaksanakan berbagai program, termasuk seminar, kegiatan bersama perguruan tinggi, dan program sertifikasi. Pada 2023, keduanya memperbarui nota kesepahaman yang mencakup perluasan kerja sama, fasilitasi pembelajaran lanjutan, dan sertifikasi profesional di bidang keamanan siber.⁴ Perkembangan ini memperlihatkan keterlibatan perusahaan teknologi asing dalam pembangunan kapasitas keamanan digital pemerintah Indonesia.

Dari sisi pertahanan, peningkatan anggaran juga menjadi bagian dari perkembangan tersebut. Pada masa pemerintahan Presiden Prabowo Subianto, anggaran pertahanan meningkat dari Rp135 triliun menjadi Rp165,2 triliun.⁵ Peningkatan anggaran ini perlu dilihat lebih lanjut dari komposisi belanjanya, terutama alokasi untuk pengadaan teknologi dan sistem pengawasan, guna mengidentifikasi sejauh mana peningkatan belanja pertahanan berkaitan dengan perkembangan ekosistem teknologi pertahanan.

Perluasan peran militer dalam ranah digital juga menjadi persoalan yang perlu dicermati. Perubahan UU TNI memperluas cakupan tugas operasi militer selain perang (OMSP), termasuk bantuan dalam menanggulangi ancaman pertahanan siber.⁶ Perluasan tugas tersebut menimbulkan pertanyaan mengenai batas kewenangan militer dalam ruang digital, terutama ketika beririsan dengan fungsi penegakan hukum dan pengawasan aktivitas masyarakat. Pernyataan pejabat TNI mengenai dugaan tindak pidana dalam unggahan Ferry Irwandi setelah demonstrasi Agustus 2025 menjadi salah satu contoh yang perlu dikaji dalam konteks batas keterlibatan militer tersebut.⁷

Selain itu, pembahasan Rancangan Undang-Undang Keamanan dan Ketahanan Siber (RUU KKS) juga memunculkan pertanyaan mengenai pembagian kewenangan pertahanan dan keamanan siber serta perlindungan hak-hak masyarakat di ruang digital. Kondisi tersebut menciptakan ekosistem yang ideal bagi berlangsungnya militerisasi teknologi, mengingat pendekatan yang digunakan dalam RUU tersebut terlalu

⁴ Indonesia Computer Security Incident Response Team Community, "Huawei dan BSSN Kerja Sama, Perkuat Keamanan Ruang Siber Nasional," <https://csirt.or.id/berita/perkuat-keamanan-ruang-siber-huawei-kerjasama-bssn>, diakses 20 Agustus 2026.

⁵ Kurnia Rahayu, "Sejalan dengan Visi Prabowo, Anggaran Pertahanan Naik Jadi Rp 165 Triliun," *Kompas.id*, 3 September 2024, <https://www.kompas.id/artikel/sejalan-dengan-visi-prabowo-anggaran-pertahanan-naik-jadi-rp-165-triliun>.

⁶ Lihat dalam UU Nomor 3 Tahun 2025.

⁷ detikNews, "Dansat Siber TNI sebut Ada Dugaan Pidana Ferry Irwandi, Konsul ke Polda Metro", <https://www.detik.com/sumut/berita/d-8102444/dansat-siber-tni-sebut-ada-dugaan-pidana-ferry-irwandi-konsul-ke-polda-metro> diakses 21 Agustus 2026

berorientasi pada keamanan negara (*state-oriented*), alih-alih berorientasi pada keamanan individu dan perlindungan warga negara.

Berbagai perkembangan tersebut memperlihatkan sejumlah aspek militerisasi teknologi di Indonesia, mulai dari keterlibatan perusahaan teknologi dalam sektor keamanan, peningkatan belanja pertahanan, hingga perluasan peran militer dalam ranah digital. Perkembangan ini menimbulkan persoalan terkait batas kewenangan militer, tata kelola dan pertanggungjawaban atas pengembangan, pengadaan, serta penggunaan teknologi, dan implikasinya terhadap HAM. Penggunaan teknologi, khususnya teknologi dwiguna, perlu dikaji tidak hanya dari segi pemanfaatannya untuk kepentingan militer, tetapi juga dari segi bagaimana teknologi tersebut dapat memperluas pengaruh dan praktik militer ke ranah sipil.

Atas dasar itu, Lembaga Studi dan Advokasi Masyarakat (ELSAM) menginisiasi penelitian mengenai militerisasi teknologi di Indonesia. Penelitian ini bertujuan memetakan ekosistem militerisasi teknologi, termasuk aktor yang terlibat, jenis teknologi, serta keterkaitan dan mekanisme pengadaannya. Penelitian ini juga mengkaji pengaturan dan mekanisme pertanggungjawaban atas pengembangan, pengadaan, dan penggunaan teknologi, serta implikasinya terhadap HAM. Secara khusus, penelitian ini menelaah upaya untuk memastikan penggunaan teknologi oleh militer tetap sesuai dengan prinsip perlindungan HAM dan mengidentifikasi tantangan serta peluang dalam mekanisme pemulihan bagi korban.

2. Rumusan Masalah

Berdasarkan latar belakang di atas, penelitian ini merumuskan beberapa pertanyaan penelitian sebagai berikut:

1. Bagaimana ekosistem militerisasi teknologi di Indonesia?
2. Bagaimana kerangka hukum dan mekanisme pengawasan serta pertanggungjawaban dalam pengembangan, pengadaan, dan penggunaan teknologi dalam konteks militerisasi teknologi di Indonesia?
3. Apa dampak militerisasi teknologi, khususnya penggunaan teknologi dwiguna , terhadap HAM?
4. Bagaimana memastikan pengembangan, pengadaan, dan penggunaan teknologi tidak memperluas praktik dan pengaruh militer yang bertentangan dengan prinsip perlindungan HAM?
5. Bagaimana tantangan dan peluang dalam mekanisme pemulihan bagi korban pelanggaran HAM yang berkaitan dengan militerisasi teknologi?

3. Metode Penelitian

Penelitian ini menggunakan pendekatan *socio-legal research*. Pendekatan ini melihat hukum tidak hanya sebagai aturan tertulis, tetapi juga dalam kaitannya dengan konteks sosial, kelembagaan, dan penerapannya dalam praktik. Dalam penelitian ini, pendekatan tersebut digunakan untuk menganalisis perkembangan militerisasi teknologi di Indonesia dengan melihat hubungan antara kebijakan, institusi, dan praktik pengembangan, pengadaan, serta penggunaan teknologi. Analisis mencakup aktor yang terlibat, alokasi sumber daya negara, serta tujuan dan konteks penggunaan teknologi.

Data penelitian diperoleh melalui studi dokumen dengan menggunakan berbagai sumber. Sumber tersebut meliputi peraturan perundang-undangan, dokumen kebijakan dan kelembagaan, laporan penelitian, publikasi akademik, pemberitaan media, serta sumber terbuka lainnya.

BAB II

TEKNOLOGI DWIGUNA, KOMPLEKS INDUSTRI-MILITER, DAN HAK ASASI MANUSIA

1. Teknologi Dwiguna

Teknologi dwiguna (*dual-use technology*) merujuk pada teknologi yang dapat dimanfaatkan untuk kepentingan sipil maupun militer. Konsep ini juga mencakup pengetahuan dan teknologi yang dapat digunakan untuk tujuan bermanfaat maupun berbahaya, termasuk yang berpotensi menimbulkan kerugian berskala besar, baik melalui pengembangan senjata maupun tanpa melibatkan proses persenjataan.⁸ Dengan demikian, teknologi dwiguna tidak hanya berkaitan dengan kemungkinan penggunaan suatu teknologi untuk kepentingan yang berbeda, tetapi juga dengan potensi dampak yang ditimbulkan dari pemanfaatannya.

Pada awalnya, istilah teknologi dwiguna banyak dikaitkan dengan material nuklir yang dapat digunakan untuk menghasilkan energi maupun mengembangkan senjata. Seiring perkembangan teknologi, cakupannya meluas hingga mencakup kecerdasan buatan (*artificial intelligence*), teknologi siber (*cyber technology*), bioteknologi (*biotechnology*), dan material maju (*advanced materials*). Perluasan ini juga berkaitan dengan semakin eratnya hubungan antara industri teknologi sipil dan sektor pertahanan. Perusahaan yang mengembangkan teknologi untuk pasar komersial dapat sekaligus memenuhi kebutuhan pemerintah dan militer. Dalam konteks ini, teknologi dwiguna tidak hanya dapat dipahami sebagai karakteristik teknologi, tetapi juga sebagai strategi pengembangan produk dan perluasan pasar.⁹

Salah satu persoalan konseptual dalam memahami teknologi dwiguna adalah luasnya cakupan istilah tersebut. Tidak semua teknologi yang digunakan untuk kepentingan sipil maupun militer serta-merta merupakan teknologi dwiguna dalam pengertian persenjataan. Internet, jaringan listrik, kamera, dan sistem komunikasi, misalnya, dapat dimanfaatkan oleh masyarakat sipil maupun militer, tetapi penggunaannya oleh militer tidak dengan sendirinya menjadikannya senjata. Oleh karena itu, perlu dibedakan antara

⁸ Miller, *Dual Use Science and Technology*.

⁹ MIT Mission Innovation X (MIx), "Defining 'Dual-Use,'" *Dual-Use Readiness Model*, <https://dualuse.mit.edu/defining-dual-use/>.

teknologi yang memiliki beragam fungsi dan teknologi yang berpotensi digunakan untuk mengembangkan senjata atau menimbulkan bahaya berskala besar.¹⁰

Persoalan ini semakin kompleks seiring dengan meningkatnya keterkaitan antara pengembangan dan penggunaan teknologi di ranah sipil dan militer. Teknologi yang dikembangkan untuk kebutuhan sipil dapat dimanfaatkan dalam sektor pertahanan, sementara teknologi yang dikembangkan untuk kepentingan militer dapat pula digunakan dalam kegiatan sipil. Keterkaitan tersebut menimbulkan tantangan dalam mengidentifikasi potensi risiko serta menentukan tanggung jawab para pengembang, pemasok, dan pengguna teknologi, terutama ketika pemanfaatannya menimbulkan dampak yang merugikan.

Dalam kaitannya dengan HAM dan demokrasi, penggunaan teknologi dwiguna berpotensi menimbulkan risiko ketika tidak disertai pembatasan kewenangan, transparansi, dan mekanisme pengawasan yang memadai. Risiko tersebut mencakup pelanggaran HAM, perluasan praktik pengawasan terhadap masyarakat, serta pembatasan kebebasan sipil yang dapat melemahkan pengawasan demokratis. Dalam konflik bersenjata, penggunaan teknologi juga harus tunduk pada prinsip perbedaan dalam hukum humaniter internasional, yang mewajibkan pihak-pihak yang berkonflik membedakan penduduk sipil dan kombatan serta objek sipil dan sasaran militer.¹¹

1.1. Jenis-Jenis Teknologi Dwiguna

1.1.1. Kecerdasan Artifisial

Kecerdasan artifisial (*Artificial Intelligence/AI*) merupakan salah satu contoh paling penting dari karakter *dual use technology* dalam perkembangan teknologi kontemporer. Perkembangan AI tidak dapat dilepaskan dari sejarah komputasi, perang, dan kebutuhan negara untuk memproses informasi secara lebih cepat. Meskipun AI saat ini sering dipahami melalui aplikasi sipil seperti mesin pencari, chatbot, sistem rekomendasi, kendaraan otomatis, atau analisis data, sebagian fondasi teknologinya memiliki hubungan yang panjang dengan kepentingan pertahanan. Hubungan ini bahkan dapat ditelusuri sejak masa Alan Turing dan Perang Dunia II.

Alan Turing merupakan salah satu figur penting dalam perkembangan ilmu komputer modern. Pada masa Perang Dunia II, Turing bekerja di Bletchley Park, pusat pemecahan sandi Inggris, dan terlibat dalam upaya memecahkan komunikasi Jerman yang dienkripsi menggunakan mesin Enigma. Turing mengembangkan metode dan perangkat

¹⁰ Miller, *Dual Use Science and Technology*.

¹¹ International Committee of the Red Cross (ICRC), "Methods and Means of Warfare," <https://www.icrc.org/en/law-and-policy/methods-and-means-warfare>,

elektromekanis yang membantu mempercepat pencarian konfigurasi Enigma, sehingga pesan-pesan militer Jerman dapat dianalisis oleh Sekutu. Namun, pekerjaan tersebut belum dapat disebut sebagai artificial intelligence dalam pengertian modern. Signifikansinya terletak pada munculnya gagasan bahwa proses penalaran dan pencarian yang sebelumnya dilakukan manusia dapat diformalkan dan dikerjakan secara sistematis oleh mesin.¹²

Setelah perang berakhir, Turing mulai mengembangkan pertanyaan yang lebih mendasar mengenai kemampuan mesin. Dalam artikelnya yang terkenal, "Computing Machinery and Intelligence" yang diterbitkan pada 1950, Turing mengajukan pertanyaan: "Can machines think?" Alih-alih berusaha mendefinisikan secara abstrak apa yang dimaksud dengan "berpikir", ia mengusulkan apa yang kemudian dikenal sebagai Imitation Game atau Turing Test, yakni suatu cara untuk menilai apakah perilaku komunikasi sebuah mesin dapat menyerupai manusia. Turing juga membahas kemungkinan munculnya *learning machines*, yaitu mesin yang tidak hanya menjalankan instruksi tetap tetapi dapat mengalami proses pembelajaran.¹³

Pemikiran Turing menjadi salah satu fondasi intelektual bagi lahirnya AI sebagai disiplin ilmu. Akan tetapi, istilah artificial intelligence sendiri baru diperkenalkan beberapa tahun kemudian. Pada 1955, John McCarthy bersama Marvin Minsky, Nathaniel Rochester, dan Claude Shannon mengajukan proposal untuk menyelenggarakan Dartmouth Summer Research Project on Artificial Intelligence. Pertemuan tersebut berlangsung pada musim panas 1956 dan kemudian dikenal sebagai salah satu tonggak kelahiran AI sebagai bidang penelitian yang berdiri sendiri. Para peneliti berangkat dari asumsi bahwa berbagai aspek pembelajaran dan kecerdasan manusia secara prinsip dapat dideskripsikan secara cukup tepat sehingga memungkinkan mesin untuk mensimulasikannya.¹⁴

Sejak awal penelitian AI juga memiliki hubungan erat dengan institusi pertahanan. Pada masa perang dingin, Amerika Serikat melihat teknologi komputasi dan otomatisasi sebagai bagian dari kompetisi strategis. Melalui Defense Advanced Research Projects Agency (DARPA), pemerintah AS kemudian membiayai berbagai penelitian mengenai interaksi manusia dan komputer, robotika, pengenalan pola, pemrosesan informasi, dan kecerdasan mesin. DARPA menyatakan bahwa investasi institusinya pada AI dapat ditelusuri sejak dekade 1960-an, termasuk penelitian mengenai hubungan simbiotik

¹² Central Intelligence Agency (CIA), "The Enigma of Alan Turing," 10 April 2015, <https://www.cia.gov/stories/story/the-enigma-of-alan-turing/>.

¹³ Sam J. Tangredi dan George Galdorisi, eds., *AI at War: How Big Data, Artificial Intelligence, and Machine Learning Are Changing Naval Warfare* (Annapolis, MD: Naval Institute Press, 2021), 51.

¹⁴ Tangredi dan Galdorisi, eds., *AI at War*, 52.

antara manusia dan mesin.¹⁵ Pada dekade 1980-an, hubungan AI dan kepentingan militer menjadi semakin eksplisit melalui *Strategic Computing Initiative*, yang berusaha mengembangkan sistem komputasi cerdas untuk berbagai kebutuhan pertahanan. Program-program pada periode ini mulai membayangkan kendaraan darat otonom, sistem bantuan bagi pilot, serta sistem manajemen pertempuran. Artinya, sejak awal perkembangan AI, kepentingan militer tidak sekadar diarahkan pada penciptaan mesin yang dapat “berpikir”, tetapi pada pertanyaan yang lebih operasional: bagaimana mesin dapat membantu militer melihat lingkungan, mengolah informasi, merencanakan tindakan, dan mempercepat pengambilan keputusan.

Salah satu penggunaan operasional AI yang penting terjadi pada Perang Teluk 1990–1991, ketika militer Amerika Serikat menggunakan *Dynamic Analysis and Replanning Tool* (DART) untuk membantu perencanaan logistik dan pergerakan personel serta perlengkapan. DART menggunakan teknik perencanaan dan penjadwalan otomatis untuk menangani persoalan transportasi militer dalam skala yang sangat kompleks. Menurut catatan DARPA, sistem tersebut memungkinkan rencana penempatan yang sebelumnya membutuhkan waktu sehari-hari dapat diselesaikan dalam hitungan jam.¹⁶ Contoh DART penting karena menunjukkan bahwa penggunaan AI dalam perang tidak selalu dimulai dari sistem yang menembakkan senjata. Sebaliknya, AI pertama-tama memperoleh nilai militer karena kemampuannya mengolah kompleksitas. AI dapat dimanfaatkan untuk mengolah informasi intelijen, mendukung perencanaan operasi dan pengambilan keputusan, serta mengoptimalkan pengelolaan logistik dan penjadwalan sumber daya.¹⁷

Perubahan yang lebih mendasar terjadi sejak akhir 2000-an dan terutama sepanjang 2010-an melalui perkembangan *machine learning*, *deep learning*, *big data*, *cloud computing*, peningkatan kapasitas semikonduktor, serta ketersediaan data digital dalam jumlah sangat besar. Tidak seperti banyak program AI pada masa Perang Dingin yang sangat bergantung pada pembiayaan pemerintah, berbagai kemajuan AI kontemporer berkembang pesat melalui industri teknologi komersial. Perusahaan teknologi mengembangkan *computer vision*, pengenalan suara, analisis data, layanan cloud, sistem navigasi, dan AI generatif untuk pasar sipil. Namun, teknologi tersebut memiliki karakter dual-use karena dapat dengan relatif cepat diadaptasi untuk kepentingan keamanan dan pertahanan. Pola inovasi karenanya mulai berubah. Jika pada masa

¹⁵ Defense Advanced Research Projects Agency (DARPA), “AI Next,” <https://www.darpa.mil/research/programs/ai-next>. DARPA menelusuri sejarah program AI-nya hingga penelitian J.C.R. Licklider pada 1960-an mengenai hubungan manusia dan kecerdasan mesin.

¹⁶ DARPA, “Breakthrough Technologies for National Security,” 2015. DART digunakan dalam Operations Desert Shield dan Desert Storm untuk mempercepat perencanaan logistik dan penempatan militer

¹⁷ Emelia Probasco, Helen Toner, Matthew Burtell, dan Tim G. J. Rudner, “AI for Military Decision-Making: Harnessing the Advantages and Avoiding the Risks,” Center for Security and Emerging Technology, April 2025, <https://doi.org/10.51593/20240028>.

sebelumnya teknologi kerap bergerak dari penelitian militer ke penerapan sipil, di era digital arah sebaliknya terjadi. Teknologi bermula dari inovasi komersial lalu diadopsi oleh militer. Perubahan tersebut menjelaskan mengapa perusahaan teknologi, penyedia cloud, produsen chip, perusahaan AI, dan *defence-tech start-up* semakin menjadi bagian dari ekosistem pertahanan, meskipun produk dasarnya tidak selalu dikembangkan sebagai senjata. Privacy International dan PAX pada 2026 bahkan menggambarkan proses tersebut sebagai konvergensi antara industri teknologi dan industri persenjataan menuju bentuk baru kompleks industri-militer (*military-industrial complex*).¹⁸

Salah satu tonggak penting menuju apa yang kemudian dikenal sebagai *algorithmic warfare* adalah pembentukan Project Maven oleh Departemen Pertahanan Amerika Serikat pada April 2017. Program ini secara formal dibentuk sebagai *Algorithmic Warfare Cross-Functional Team* untuk mempercepat integrasi big data, AI, dan machine learning dalam operasi pertahanan. Pada tahap awal, Project Maven diarahkan untuk mengatasi persoalan yang sangat konkret: militer memiliki volume rekaman dan citra dari sistem intelligence, surveillance and reconnaissance (ISR) yang terlalu besar untuk dianalisis secara manual oleh manusia. Algoritma computer vision kemudian digunakan untuk membantu mendeteksi dan mengklasifikasikan objek dalam citra dan video, sehingga analisis dapat mengubah data dalam jumlah besar menjadi informasi yang dapat digunakan dalam operasi. Departemen Pertahanan AS menggambarkan tujuannya sebagai upaya mengubah volume data yang besar menjadi actionable intelligence.⁷ Perubahan tersebut penting karena algoritma mulai ditempatkan di antara sensor dan keputusan manusia: teknologi tidak lagi sekadar mengumpulkan informasi, tetapi turut menentukan informasi mana yang dianggap relevan, objek apa yang harus diperhatikan, dan ancaman mana yang perlu diprioritaskan.

Dalam pengertian tersebut, *algorithmic warfare* dapat dipahami sebagai bentuk peperangan di mana algoritma semakin digunakan untuk memproses informasi, mengenali pola, mengklasifikasikan objek, menghasilkan prediksi atau rekomendasi, dan mempercepat proses pengambilan keputusan dalam operasi militer. AI dapat hadir di hampir seluruh rantai operasi: pengumpulan data melalui sensor; pengolahan citra satelit atau drone; pengenalan objek; identifikasi potensi ancaman; penentuan prioritas; rekomendasi tindakan kepada komandan; hingga integrasinya dengan sistem persenjataan. Perkembangan Project Maven menunjukkan bagaimana fungsi tersebut semakin dekat dengan proses targeting. Laporan Government Accountability Office (GAO) pada 2022, misalnya, mencatat pengembangan kemampuan target recognition melalui Scarlet Dragon, yang menggunakan data Project Maven. Dalam demonstrasi live-fire pada Oktober 2021, kemampuan AI tersebut digunakan lintas platform Angkatan

¹⁸ Privacy International dan PAX, *Tech Giants, the Arms Industry and the Weaponisation of AI: When Algorithms Go to War*, June 2026.

Darat, Angkatan Udara, dan Angkatan Laut untuk membantu mengidentifikasi target yang kemudian diserang.¹⁹ Dengan demikian, persoalan penting dalam algorithmic warfare bukan semata-mata apakah AI secara otomatis “memutuskan membunuh”, tetapi bagaimana AI semakin terintegrasi dalam proses *find, identify, track, target, engage and assess*, yang sebelumnya sangat bergantung pada penilaian manusia.

Meski demikian, AI tidak boleh disamakan begitu saja dengan *autonomous weapons*. Tidak semua sistem senjata otonom menggunakan AI, dan tidak semua penggunaan AI oleh militer merupakan sistem persenjataan. ICRC membedakan beberapa aplikasi utama AI dalam konflik bersenjata: penggunaan AI untuk meningkatkan otonomi dalam sistem robotik, termasuk senjata; penggunaan AI dalam operasi siber dan informasi; serta penggunaan AI sebagai *decision-support system*.²⁰ AI juga dapat digunakan untuk logistik, pemeliharaan prediktif, navigasi, intelijen, surveilans, atau pengelolaan informasi tanpa secara langsung menyerang target. Namun, semakin dekat AI ditempatkan pada keputusan yang menentukan siapa atau apa yang menjadi sasaran, semakin serius pula pertanyaan mengenai kontrol manusia, reliabilitas, bias, transparansi, dan akuntabilitas. Pemerintah Amerika Serikat sendiri melalui DoD Directive 3000.09 mensyaratkan bahwa sistem senjata otonom dan semi-otonom harus dirancang agar komandan dan operator dapat menjalankan tingkat penilaian manusia yang sesuai atas penggunaan kekuatan. ICRC juga menekankan pentingnya mempertahankan human judgement, khususnya ketika sistem AI digunakan dalam keputusan yang membawa konsekuensi serius terhadap kehidupan manusia.

Karakter *dual-use* AI pada akhirnya membuat algorithmic warfare memiliki konsekuensi yang melampaui medan perang. Teknologi pengenalan wajah, analisis perilaku, geolokasi, penggabungan basis data, *computer vision*, dan pemrosesan biometrik dapat berpindah antara konteks militer, keamanan, perbatasan, kepolisian, dan pengawasan domestik. ICRC memperingatkan bahwa penggunaan AI dapat memungkinkan penggabungan data dari sensor, komunikasi, basis data, media sosial, dan data biometrik untuk menghasilkan penilaian algoritmik mengenai individu, termasuk status atau potensi tindakannya. Privacy International juga menyoroti bahwa teknologi berbasis data yang digunakan dalam peperangan dapat sekaligus menopang *mass surveillance* dan perluasan *surveillance state*.²¹ Artinya, AI sebagai dual-use technology tidak hanya mengaburkan batas antara teknologi sipil dan militer pada tingkat produk, tetapi juga

¹⁹ U.S. Department of Defense, “Project Maven to Deploy Computer Algorithms to War Zone by Year’s End,” 21 Juli 2017; dan “Project Maven Industry Day Pursues Artificial Intelligence for DoD Challenges,” 3 November 2017.

²⁰ International Committee of the Red Cross (ICRC), *Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach*, June 2019.

²¹ International Committee of the Red Cross (ICRC), “FAQ: Artificial Intelligence (AI) in the Military Domain,” 11 Juni 2026, <https://www.icrc.org/en/article/faq-artificial-intelligence-in-military-domain>; Privacy International dan PAX, *Tech Giants, the Arms Industry and the Weaponisation of AI: When Algorithms Go to War*.

dapat mengaburkan batas antara medan perang dan ruang sipil. Karena itu, analisis terhadap militerisasi AI perlu memperhatikan bukan hanya teknologi yang digunakan dan kemampuan yang dihasilkannya, tetapi juga perusahaan yang mengembangkannya, data yang digunakan untuk melatih dan menjalankan sistem, infrastruktur digital yang menopangnya, mekanisme pengadaan, serta sejauh mana keputusan berbasis algoritma tetap dapat dipertanggungjawabkan secara hukum dan demokratis.

1.1.2. Unmanned Aerial Vehicles (UAVs)

Unmanned Aerial Vehicles (UAVs) atau drone merupakan salah satu teknologi yang banyak digunakan oleh militer maupun kelompok bersenjata non-negara di wilayah konflik. Namun, drone juga memiliki karakter sebagai teknologi dwiguna karena dapat dimanfaatkan untuk berbagai kepentingan sipil, termasuk oleh perusahaan multinasional, lembaga kemanusiaan, serta tim tanggap darurat untuk pemetaan, pemantauan bencana, distribusi bantuan, dan berbagai kebutuhan lain yang mendukung kepentingan masyarakat.

Di sisi lain, drone juga digunakan untuk kepentingan intelijen, pengawasan, serta pendokumentasian pelanggaran hak asasi manusia. Dalam konteks militer, drone dapat digunakan untuk memantau individu atau kelompok tertentu yang dianggap memiliki profil atau kepentingan strategis. Data yang dikumpulkan melalui pengawasan tersebut selanjutnya dapat diolah dan dimasukkan ke dalam daftar target (*target lists*), baik yang disusun oleh manusia maupun dengan bantuan sistem algoritmik. Daftar tersebut kemudian dapat digunakan untuk menentukan lokasi atau sasaran operasi serangan menggunakan drone berjenis Medium Altitude Long Endurance (MALE) maupun sistem *loitering munition* yang lebih kecil.²²

Karakter tersebut menunjukkan bahwa drone memiliki fungsi strategis yang sangat beragam. Di satu sisi, drone merupakan teknologi yang relatif fleksibel dan mudah diakses serta menawarkan berbagai manfaat bagi masyarakat. Namun, di sisi lain, teknologi yang sama dapat diintegrasikan ke dalam sistem persenjataan jarak jauh untuk melakukan pengawasan, identifikasi sasaran, hingga serangan mematikan. Dengan demikian, drone menjadi salah satu contoh paling jelas mengenai bagaimana teknologi dual-use dapat bergerak dari fungsi sipil dan kemanusiaan menuju fungsi pengawasan, intelijen, dan penggunaan kekuatan dalam konteks militer.

Penggunaan drone dalam operasi militer memunculkan persoalan etika karena memungkinkan serangan dilakukan dengan risiko yang jauh lebih kecil bagi militer dari

²²James Patton Rogers, "Introduction: Why Study Drones?," dalam *De Gruyter Handbook of Drone Warfare*, ed. James Patton Rogers (Berlin/Boston: De Gruyter, 2024), 2.

negara pengguna. UAVs ini kerap dipandang sebagai sarana untuk melakukan serangan secara lebih presisi dan efisien. Namun, kemudahan melakukan operasi dari jarak jauh juga memunculkan perdebatan mengenai batas penggunaan kekuatan, legitimasi penargetan, serta perlindungan terhadap penduduk sipil.²³

Menurut temuan SIPRI yang dirilis pada April 2026, tren belanja militer global menunjukkan adanya pergeseran baik dari sisi skala maupun distribusi geografis. Belanja militer global meningkat dari 2,4 persen terhadap PDB dunia pada menjadi 2,5 persen pada 2025, dengan rata-rata belanja militer mencapai 6,9 persen dari total pengeluaran pemerintah dan sekitar US\$352 per kapita. Menariknya, peningkatan belanja global tetap terjadi meskipun pengeluaran militer Amerika Serikat mengalami penurunan. Pertumbuhan belanja yang tajam di Eropa serta peningkatan berkelanjutan di Asia dan Oseania mampu mengimbangi penurunan tersebut; bahkan, jika Amerika Serikat dikeluarkan dari perhitungan, belanja militer dunia meningkat sebesar 9,2 persen pada 2025.

Pergeseran ini juga menunjukkan semakin besarnya porsi anggaran yang diarahkan pada teknologi dan kapasitas militer modern. India, misalnya, meningkatkan belanja militernya sebesar 8,9 persen menjadi US\$92,1 miliar, terutama setelah konflik dengan Pakistan pada Mei 2025 yang melibatkan pesawat tempur, drone, dan rudal. Sementara itu, Iran meningkatkan secara signifikan pendanaan bagi industri domestik yang memproduksi pesawat militer, drone, dan rudal balistik. Perkembangan ini memperlihatkan bahwa peningkatan belanja pertahanan tidak hanya berkaitan dengan jumlah anggaran, tetapi juga dengan penguatan industri pertahanan dan investasi pada teknologi seperti drone, sistem udara, dan rudal. Pada saat yang sama, keberadaan mekanisme pembiayaan di luar anggaran resmi, seperti yang ditemukan dalam program drone dan rudal Iran, turut menunjukkan tantangan transparansi dalam mengukur secara utuh skala belanja militer.²⁴

Penggunaan drone komersial oleh militer Israel dalam operasi di Gaza menunjukkan bagaimana teknologi yang pada awalnya dikembangkan untuk kepentingan sipil dapat mengalami proses militerisasi dan weaponization. DJI, perusahaan teknologi asal Tiongkok yang dikenal sebagai salah satu produsen utama drone komersial dunia, pada dasarnya mengembangkan produknya untuk berbagai kepentingan sipil, seperti fotografi, pemetaan, pertanian dan inspeksi. Namun, drone yang diproduksi oleh DJI ini juga telah digunakan oleh Israel untuk kepentingan militer setidaknya sejak sebelum perang Gaza 2023. Investigasi Bellingcat tahun 2018, menemukan adanya penggunaan sejumlah

²³ Rogers, "Introduction: Why Study Drones?," 10.

²⁴ Xiao Liang, Nan Tian, Diego Lopes da Silva, Lorenzo Scarazzato, Zubaida Karim, dan Jade Guiberteau Ricard, "Trends in World Military Expenditure, 2025," *SIPRI Fact Sheet* (Stockholm International Peace Research Institute (SIPRI), April 2026), 1.

drone komersial DJI, termasuk Matrice 100 dan Matrice 600, oleh Israel di sekitar Gaza. DJI Matrice 600 ketika itu dimodifikasi dengan mekanisme yang memungkinkan pelepasan beberapa granat gas air mata terhadap demonstran dalam aksi Great March of Return²⁵

Penggunaan drone komersial tersebut semakin berkembang setelah pecahnya perang Gaza pada Oktober 2023. Pada April 2024, media Israel Globes melaporkan bahwa Israel Defense Forces (IDF) memesan ribuan drone produksi DJI dan Autel Robotics yang diperuntukkan bagi pencitraan dan pengintaian jarak dekat, termasuk untuk memperoleh informasi intelijen dalam operasi di Gaza²⁶. Perkembangan ini memperlihatkan bahwa drone komersial dapat mengisi kebutuhan operasional militer tanpa harus melalui pengembangan platform UAV khusus. Harga yang relatif lebih murah, ketersediaan komersial, kemampuan kamera, serta fleksibilitas operasional menjadikan drone sipil dapat dengan cepat diadaptasi untuk fungsi intelligence, surveillance and reconnaissance (ISR).

Fungsi tersebut kemudian dilaporkan berkembang dari pengawasan menuju penggunaan yang lebih langsung dalam operasi tempur. Investigasi unit verifikasi Sanad milik Al Jazeera yang diterbitkan pada Mei 2025 menemukan indikasi bahwa beberapa jenis drone DJI telah dimodifikasi oleh militer Israel untuk berbagai fungsi dalam operasi di Gaza, beberapa diantaranya (1) DJI Mavic dilaporkan digunakan untuk pengintaian dan target acquisition, (2) DJI Avata, drone kecil yang pada dasarnya dirancang untuk perekaman video, digunakan untuk menavigasi dan memetakan jaringan terowongan, (3) DJI Agras, drone yang dirancang untuk kepentingan pertanian dimodifikasi dan digunakan untuk menjatuhkan bahan peledak ke sebuah bangunan organisasi kemanusiaan IHH di Jabalia pada Juli 2025 serta penggunaannya dalam serangan lain di Beit Lahia.²⁷

1.1.3. Teknologi Pengawasan dan Biometrik.

Teknologi pengawasan (*surveillance technology*) tidak terbatas pada teknologi pengenalan wajah (*facial recognition*) atau biometrik, tetapi mencakup berbagai perangkat dan sistem yang memungkinkan negara maupun aktor lain untuk mengumpulkan, mengakses, mengintersepsi, mengidentifikasi, melacak, menganalisis,

²⁵ Nick Waters, "First ISIS, then Iraq, now Israel: IDF Use of Commercial Drones," *Bellingcat*, 18 Juni 2018, <https://www.bellingcat.com/news/middle-east/2018/06/18/first-isis-iraq-now-israel-idf-use-commercial-drones/>, diakses 3 September 2026.

²⁶ Assaf Gilead, "IDF Procurement of Chinese Drones Raises Concerns," *Globes*, 25 April 2024. <https://en.globes.co.il/en/article-idf-procurement-of-chinese-drones-raises-concerns-1001477502>

²⁷ Al Jazeera, "Israel Retrofitting DJI Commercial Drones to Bomb and Surveil Gaza," 8 Mei 2025, <https://www.aljazeera.com/news/2025/5/8/israel-retrofitting-dji-commercial-drones-to-bomb-and-surveil-gaza>, diakses 5 September 2026.

informasi mengenai individu, kelompok, komunikasi, maupun suatu wilayah. Teknologi pengawasan dibedakan menjadi *network surveillance*, yaitu pengawasan yang dilakukan melalui infrastruktur jaringan telekomunikasi dan *tactical surveillance* yang memungkinkan akses secara langsung terhadap perangkat seseorang secara jarak jauh seperti IMSI Catchers dan Intrusion Technologies.

Dalam perkembangannya, ekosistem ini juga mencakup *spyware*, sistem geolokasi, CCTV, facial recognition, pengawasan media sosial, *mobile phone extraction*, *drone surveillance*, serta sistem analisis berbasis AI. Dalam konteks pertahanan, surveilans sejak lama merupakan bagian dari fungsi intelijen, khususnya melalui konsep *intelligence, surveillance and reconnaissance* (ISR). Namun, digitalisasi telah mengubah skala dan karakter pengawasan tersebut. Pengawasan tidak lagi hanya dilakukan dengan mengamati suatu objek atau menyadap komunikasi tertentu, tetapi semakin bergantung pada pengumpulan dan penggabungan data dalam jumlah besar, termasuk metadata komunikasi, lokasi, data biometrik, aktivitas sosial media, citra satelit maupun drone, dan data dari berbagai sensor. Privacy International menggambarkan data sebagai unsur sentral dalam militerisasi teknologi kontemporer karena sistem berbasis data memungkinkan negara mendeteksi pola perilaku, memetakan hubungan antar manusia, mengidentifikasi aktivitas yang dianggap menyimpang bahkan membantu membentuk target untuk operasi keamanan atau militer.²⁸ Proses militerisasi dengan demikian terjadi bukan hanya ketika sebuah kamera atau perangkat lunak secara langsung digunakan di medan perang, tetapi juga ketika data yang dikumpulkan digunakan untuk fungsi intelijen, identifikasi ancaman, penargetan, dan pengambilan keputusan keamanan.

Salah satu bentuk pengawasan yang paling intrusif adalah *spyware*, ia bekerja dengan cara memperoleh akses secara tersembunyi ke perangkat digital target atau korban. Contohnya adalah Pegasus yang dikembangkan oleh NSO Group, dapat mengakses pesan, surat elektronik, kontak, panggilan, mikrofon, kamera, dan berbagai data lainnya pada perangkat korban secara real-time. Dalam riset ELSAM berjudul *Privasi dalam Rumah Kaca: Menggugat Akuntabilitas Spyware di Indonesia*, institusi militer setidaknya telah menghabiskan anggaran sebesar 1.3 triliun rupiah untuk pengadaan teknologi surveilans yang tidak jelas bagaimana proses pengadaannya dan untuk apa teknologi tersebut digunakan. Investigasi Amnesty International dan Citizen Lab telah mendokumentasikan mayoritas penggunaan Pegasus menyasar pada jurnalis, pembela HAM, aktivis, dan aktor masyarakat sipil di berbagai negara. Di Palestina, misalnya, analisis forensik yang ditinjau secara independen oleh Amnesty International dan Citizen Lab mengonfirmasi bahwa enam perangkat milik pembela HAM Palestina telah terinfeksi

²⁸ Privacy International, "What Is Militarisation of Tech?," 2025, <https://privacyinternational.org/long-read/5668/what-militarisation-tech>, diakses 7 September 2026.

Pegasus pada 2020–2021.²⁹ Kasus-kasus tersebut memperlihatkan bagaimana teknologi yang dipasarkan untuk kepentingan pemberantasan terorisme atau pencarian DPO berpotensi digunakan terhadap pihak yang tidak terkait dengan ancaman keamanan.

Selain melalui *spyware*, pengawasan juga dapat dilakukan tanpa meretas perangkat target secara langsung. Sistem *lawful interception*, misalnya, memungkinkan otoritas memperoleh komunikasi melalui infrastruktur operator telekomunikasi, sementara IMSI catcher bekerja dengan menyamar sebagai menara seluler sehingga perangkat di sekitarnya terkoneksi dan mengungkap identitas jaringan serta informasi lokasinya. Beberapa jenis IMSI catcher juga dapat mengintersepsi komunikasi, sehingga penggunaannya di lokasi demonstrasi atau pertemuan politik dapat mengumpulkan data tidak hanya dari individu yang menjadi target tetapi juga orang lain di sekitarnya.³⁰ Selain *spyware* dan IMSI Catcher, ada beberapa teknologi surveilans lain seperti (1) facial recognition yang dapat digunakan untuk mengidentifikasi seseorang dari kamera publik, (2) social media monitoring dapat memetakan aktivitas, jaringan pertemanan, atau pandangan politik, (3) data lokasi dapat memperlihatkan pergerakan, (4) mobile phone extraction dapat memperoleh data dari telepon yang telah disita. Informasi tersebut kemudian dapat digabungkan dengan basis data dan dianalisis melalui sistem AI untuk membentuk profil, watchlist, atau penilaian risiko terhadap individu tertentu.

2. Kompleks Militer-Industri, Konteks Indonesia

Konsep kompleks industri-militer (*military-industrial complex/MIC*) pada dasarnya digunakan untuk menjelaskan hubungan struktural antara institusi militer, pemerintah, dan industri yang memperoleh kepentingan ekonomi dari pembangunan serta pemeliharaan kekuatan pertahanan. Karena itu, MIC sebaiknya tidak dipahami secara sempit sebagai sekadar “kerja sama antara militer dan perusahaan senjata.” Konsep tersebut menunjuk pada suatu ekosistem kepentingan di mana kebutuhan keamanan menghasilkan anggaran, penelitian, pengadaan dan kontrak; industri memperoleh pasar dari kebutuhan tersebut; sementara kapasitas industri dan perkembangan teknologi pada gilirannya dapat memengaruhi cara negara mendefinisikan kebutuhan pertahanannya. Bahkan sebelum istilah MIC diperkenalkan oleh Dwight D. Eisenhower, C. Wright Mills dalam *The Power Elite* (1956) telah mengidentifikasi semakin bertautnya elite politik, korporasi besar, dan militer di Amerika Serikat. Menurut Mills, perkembangan institusi-

²⁹ Amnesty International Security Lab dan Citizen Lab, “Devices of Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware,” 8 November 2021. <https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/> diakses pada 7 September 2026

³⁰ Tim Privacy International dan ELSAM, *Privasi 101: Panduan Memahami Privasi, Perlindungan Data, dan Surveilans Komunikasi* (Jakarta: ELSAM dan Privacy International, 2015), 46.

institusi besar tersebut menghasilkan struktur kekuasaan di mana keputusan ekonomi, politik dan militer semakin sulit dipisahkan satu sama lain.³¹

Perkembangan MIC tidak dapat dilepaskan dari transformasi peperangan selama Perang Dunia II dan Perang Dingin. Perang Dunia II memobilisasi tidak hanya tentara, tetapi juga perusahaan, universitas, ilmuwan, laboratorium dan kapasitas produksi industri untuk menghasilkan pesawat, radar, komunikasi, roket, komputer, hingga senjata nuklir. Struktur tersebut tidak sepenuhnya dibongkar setelah perang berakhir. Thomas C. Lassman menunjukkan bahwa pada 1946, ketika masih menjabat sebagai Kepala Staf Angkatan Darat Amerika Serikat, D. Eisenhower membentuk divisi research and development di War Department untuk mempercepat inovasi persenjataan dan mempertahankan keunggulan teknologi militer. Perang Dingin kemudian membuat hubungan negara dengan militer dan industri tersebut semakin permanen karena adanya kompetisi dengan Uni Soviet membutuhkan pengeluaran pertahanan, penelitian teknologi, dan produksi persenjataan secara terus menerus. Dengan demikian, terbentuknya hubungan jangka panjang antara *military demand*, *public funding*, *technological research* dan *industrial production*.³²

Menurut Eisenhower, pertemuan antara institusi militer yang sangat besar dan industri persenjataan menciptakan kekuatan ekonomi dan politik baru yang berpotensi memunculkan pengaruh yang tidak semestinya (*unwarranted influence*) dalam proses pemerintahan. Yang sering luput adalah bahwa Eisenhower juga menghubungkan perubahan tersebut dengan revolusi teknologi yang di mana penelitian menjadi semakin mahal, kompleks dan bergantung pada pendanaan serta pengarahan pemerintah.

Pada abad ke-21, perkembangan teknologi digital telah mengubah karakter pertahanan dan keamanan kontemporer. Kapabilitas militer tidak lagi semata-mata ditentukan oleh kepemilikan persenjataan konvensional seperti senapan, tank, kapal perang dan pesawat tempur, tetapi semakin bergantung pada kecerdasan artifisial, sistem pengawasan, pesawat tanpa awak (*unmanned aerial vehicle*), satelit, pengolahan data dan lain sebagainya. Perubahan ini sekaligus mengaburkan batas antara teknologi sipil dan teknologi militer karena sebagian teknologi tersebut bersifat *dwiguna*, dikembangkan atau digunakan untuk kepentingan sipil, tetapi dapat diadaptasi untuk kepentingan pertahanan, intelijen dan operasi militer. Selain itu, perubahan serupa dapat diamati dalam perkembangan kebijakan pertahanan Indonesia. Komite Kebijakan Industri Pertahanan (KKIP), misalnya menetapkan sepuluh teknologi kunci sebagai program

³¹ C. Wright Mills, *The Power Elite* (New York: Oxford University Press, 1956), 275.

³² Thomas C. Lassman, "Putting the Military Back into the History of the Military-Industrial Complex: The Management of Technological Innovation in the U.S. Army, 1945–1960," *Isis* 106, no. 1 (2015): 94–120, <https://doi.org/10.1086/681038>.

prioritas industri pertahanan dan beberapa di antaranya adalah *unmanned aerial vehicle* dan satelit militer. Disaat yang sama, Kementerian Pertahanan dan TNI mulai memberikan perhatian besar terhadap AI, cyber defence, sistem nirawak dan integrasi berbagai sensor platform.³³

Perkembangan tersebut menunjukkan bahwa militerisasi teknologi perlu dilihat sebagai sebuah ekosistem, bukan sekadar proses pengadaan alat utama sistem senjata (alutsista). Ekosistem tersebut setidaknya terdiri atas empat unsur yang saling berkaitan yaitu teknologi, institusi militer dan negara, industri pertahanan dan perusahaan swasta serta mekanisme anggaran dan pengadaan. Deikin menunjukkan bahwa produksi persenjataan tidak hanya ditentukan oleh kebutuhan pertahanan, tetapi juga oleh kepentingan ekonomi aktor-aktor yang memperoleh keuntungan dari keberlanjutan produksi dan pengadaan senjata. Dalam kerangka kompleks industri-militer, kepentingan tersebut dapat membentuk hubungan yang saling memperkuat: persepsi ancaman mendorong peningkatan anggaran dan pengadaan; pengadaan menciptakan pasar bagi industri; sementara keberadaan kapasitas industri dan kepentingan ekonomi yang telah terbentuk dapat turut mendorong keberlanjutan permintaan terhadap teknologi pertahanan. Karena itu, kompleks militer-industri tidak cukup dipahami sebagai hubungan kontraktual antara militer dan perusahaan, melainkan sebagai suatu ekosistem di mana kepentingan keamanan, kebijakan negara, anggaran publik, industri, dan perkembangan teknologi saling berkelindan.³⁴

Terlebih lagi, hal ini juga didukung dengan adanya lonjakan anggaran pertahanan di seluruh dunia, Menurut Stockholm International Peace Research Institute (SIPRI), belanja militer dunia pada tahun 2024 mencapai US\$2.7 triliun, meningkat 9.4% dari tahun sebelumnya, ini merupakan kenaikan tahunan tertinggi sejak berakhirnya perang dingin.³⁵ Salah satu negara yang mengalami lonjakan tersebut adalah Indonesia. Pada 10 Juni 2026 Menteri Pertahanan Sjafrie Sjamsoeddin menyampaikan kepada Komisi I DPR RI bahwa kebutuhan ideal anggaran pertahanan untuk tahun 2027 mencapai Rp667 triliun, jauh melampaui pagu indikatif yang ditetapkan oleh Kementerian Keuangan dan Bappenas sebesar Rp139 triliun. Kementerian Pertahanan kemudian mengajukan tambahan anggaran sebesar Rp195 triliun, sehingga total usulan riil ke DPR menjadi

³³ Komite Kebijakan Industri Pertahanan (KKIP), "Rencana Aksi Industri Pertahanan: Penguasaan Sepuluh Teknologi Prioritas," 20 Februari 2023, <https://www.kkip.go.id/2023/02/20/rencana-aksi-industri-pertahanan-penguasaan-sepuluh-teknologi-prioritas/>.

³⁴ Alexander Deikin, *An Alliance of the Monopolies and the Military: On the US Military-Industrial Complex* (Moscow: Novosti Press Agency, 1973), 20.

³⁵ Stockholm International Peace Research Institute (SIPRI), "Unprecedented Rise in Global Military Expenditure as European and Middle East Spending Surges," *Press Release*, 28 April 2025, <https://www.sipri.org/media/press-release/2025/unprecedented-rise-global-military-expenditure-european-and-middle-east-spending-surges>.

Rp334 triliun untuk mendukung modernisasi alutsista dan pembangunan kekuatan pertahanan.³⁶

Salah satu karakter utama militerisasi teknologi kontemporer adalah semakin kaburnya pemisahan antara teknologi sipil dan militer. Fenomena ini dapat dijelaskan melalui konsep teknologi dwiguna. Drone merupakan contoh paling jelas. Drone dapat digunakan untuk pemetaan wilayah, pertanian, pemantauan bencana, fotografi, dan pengiriman barang. Namun, platform dan teknologi serupa dapat digunakan untuk pengintaian (*reconnaissance*), pengawasan (*surveillance*), akuisisi target, pengiriman amunisi, bahkan serangan. Kementerian Pertahanan sendiri mengakui karakter *dual-use* drone serta perannya sebagai salah satu teknologi yang mengubah peperangan modern.³⁷ AI memperbesar persoalan tersebut. Algoritma *computer vision*, misalnya, dapat digunakan untuk mengenali objek dalam penggunaan komersial, tetapi juga dapat diintegrasikan ke dalam sistem pengawasan untuk mengidentifikasi orang, kendaraan, atau target. Infrastruktur cloud yang digunakan perusahaan dan lembaga pemerintah dapat pula digunakan untuk penyimpanan dan pemrosesan data pertahanan. Sistem komunikasi satelit dapat melayani komunikasi sipil sekaligus operasi militer.

Perkembangan tersebut sudah terlihat dalam orientasi pertahanan Indonesia tetapi konsep MIC yang digaungkan oleh Eisenhower perlu digunakan secara hati-hati karena struktur industri pertahanan Indonesia berbeda dengan Amerika Serikat. Jika MIC klasik Amerika banyak ditopang hanya dengan perusahaan pertahanan swasta, dalam kasus Indonesia, industri pertahanan Indonesia secara historis memiliki peran negara, BUMN dan perusahaan swasta yang jauh lebih dominan. Akar industrinya bahkan dapat ditelusuri ke masa kolonial, cikal bakal PT Pindad berasal dari Constructie Winkel yang didirikan pada 1808, PT PAL berakar pada Marine Establishment pada 1939, sedangkan sejarah industri penerbangan yang kemudian berkembang menjadi PT Dirgantara Indonesia dapat ditelusuri ke fasilitas penerbangan Hindia Belanda pada awal abad ke-20.³⁸ Pasca-kemerdekaan, perusahaan-perusahaan tersebut mengalami nasionalisasi dan reorganisasi hingga menjadi bagian dari industri strategis negara. Dalam perkembangannya, orientasi industri pertahanan Indonesia tidak hanya diarahkan untuk memenuhi kebutuhan TNI dan Polri, tetapi juga untuk memasuki pasar pertahanan

³⁶ Tempo, "Menhan: Kebutuhan Anggaran Pertahanan Tahun 2027 Rp 667 Triliun," <https://www.tempo.co/politik/menhan-kebutuhan-anggaran-pertahanan-tahun-2027-rp-667-triliun-2266159>, diakses 3 Juli 2026.

³⁷ Gede Priana Dwipratama, "Swarm Drone: Tantangan, Peluang dan Ancaman bagi Indonesia," Direktorat Jenderal Potensi Pertahanan Kementerian Pertahanan Republik Indonesia, 25 April 2024, <https://www.kemhan.go.id/pohtan/2024/04/25/swarm-drone-tantangan-peluang-dan-ancaman-bagi-indonesia.html>.

³⁸ Komite Kebijakan Industri Pertahanan (KKIP), "Sejarah Industri Pertahanan Nasional," <https://www.kkip.go.id/sejarah>.

International. PT Pindad misalnya, memproduksi senjata, amunisi dan kendaraan khusus untuk kebutuhan pertahanan nasional sekaligus untuk mencari uang dari negara lain.

Perusahaan tersebut secara resmi menyebut Myanmar sebagai salah satu negara yang pernah menjadi tujuan ekspor produknya, bersama Malaysia, Brunei Darussalam, Timor-Leste, Singapura, Bangladesh, Laos, Thailand, Korea Selatan, dan Amerika Serikat.³⁹ Namun, keberadaan Myanmar dalam daftar negara tujuan ekspor tidak dengan sendirinya menunjukkan bahwa produk tersebut dijual kepada junta setelah kudeta Februari 2021. DEFEND ID menyatakan bahwa ekspor PT Pindad ke Myanmar dilakukan pada 2016 berupa amunisi spesifikasi olahraga untuk keperluan ASEAN Armies Rifle Meet (AARM), serta membantah adanya ekspor produk pertahanan PT Pindad ke Myanmar setelah kudeta 2021.

Persoalan akuntabilitas kemudian mengemuka pada Oktober 2023 ketika Chin Human Rights Organisation (CHRO), Myanmar Accountability Project (MAP), dan mantan Jaksa Agung Indonesia Marzuki Darusman mengajukan pengaduan kepada Komnas HAM mengenai dugaan penjualan produk pertahanan oleh PT Pindad, PT PAL, dan PT Dirgantara Indonesia kepada militer Myanmar.⁴⁰ Para pengadu mendalilkan adanya promosi dan dugaan transfer senapan, pistol, amunisi, kendaraan tempur, serta peralatan militer lainnya selama sekitar satu dekade, termasuk kemungkinan transaksi setelah kudeta Februari 2021. Komnas HAM mengonfirmasi penerimaan pengaduan tersebut dan menyatakan akan melakukan telaah untuk menentukan ada atau tidaknya dugaan pelanggaran HAM, sekaligus mempertimbangkan persoalan kewenangan karena perkara melibatkan pihak di luar Indonesia.

Selain mengekspor, teknologi dwiguna ini juga sudah semakin banyak digunakan di Indonesia. Pada 2024, TNI Angkatan Udara menyatakan telah menggunakan AI dalam latihan pertahanan udara dan berencana memperluas pengembangan teknologi AI dan siber. Sistem Pertahanan Udara Nasional "Cakra" bahkan dirancang untuk mengintegrasikan sensor, shooter, dan command and control (C2), dengan AI digunakan untuk mempercepat proses pengambilan keputusan. Arsitektur tersebut mencakup *integrated air defence, electromagnetic warfare, cyber and space*, serta integrasi platform laut, udara, dan darat. Pengembangan PTTA MALE "Elang Hitam" juga menggambarkan

³⁹ PT Pindad (Persero), "Kendarai Ranops Maung, Presiden Tinjau Divisi Munisi dan Apresiasi Kemampuan Lini Produksi PT Pindad," 27 Juli 2023, <https://pindad.com/kendarai-ranops-maung-presiden-tinjau-divisi-munisi-dan-apresiasi-kemampuan-lini-produksi-pt-pindad>.

⁴⁰ Chin Human Rights Organisation (CHRO) dan Myanmar Accountability Project (MAP), "Indonesian Arms Producers Accused of Illegal Sales to Myanmar," 2 Oktober 2023, <https://progressivevoicemyanmar.org/2023/10/02/press-release-indonesian-arms-producers-accused-of-illegal-sales-to-myanmar>. Pengaduan tersebut menyebut PT Pindad, PT PAL, dan PT Dirgantara Indonesia serta dugaan penjualan berbagai produk pertahanan kepada militer Myanmar

kecenderungan tersebut.⁴¹ Program ini melibatkan konsorsium yang terdiri antara lain dari Kemhan, TNI AU, PT Dirgantara Indonesia, PT LEN, serta lembaga penelitian dan universitas, dengan orientasi integrasi UAV dengan sistem persenjataan dan C4ISR.

Dalam operasi keamanan di Papua, TNI telah menggunakan drone terutama untuk pengawasan, pengintaian, dan penyisiran awal wilayah operasi yang alasannya adalah untuk mengurangi risiko terhadap personal. Panglima TNI Jenderal Agus Subiyanto pada Desember 2023, menyatakan bahwa drone digunakan untuk memantau rute dan kondisi wilayah sebelum pasukan bergerak masuk ke daerah yang dianggap rawan. Pada 2024, Korps Marinir juga menyiapkan DJI Enterprise Matrice 350 RTK dan DJI Enterprise Matrice 30 Series untuk mendukung Satgas Pengamanan Perbatasan Mobile Indonesia Papua Nugini; kedua drone tersebut merupakan produk DJI, perusahaan teknologi asal Tiongkok, dan diuji untuk kemampuan mendeteksi serta mengikuti pergerakan kendaraan maupun personel secara terus-menerus di medan operasi. Seri M30 juga dapat dilengkapi kamera wide, zoom, dan thermal, sehingga dapat digunakan untuk pengawasan dan identifikasi target dalam kondisi medan yang sulit.⁴²

Dengan demikian, militerisasi teknologi tidak harus dipahami sebagai penciptaan teknologi yang sejak awal eksklusif untuk militer. Militerisasi juga berlangsung ketika teknologi, keahlian, data, dan infrastruktur yang memiliki fungsi sipil diintegrasikan ke dalam fungsi pertahanan dan keamanan. Hal ini menghasilkan pertanyaan tata kelola yang lebih kompleks. Regulasi yang berorientasi pada "senjata" atau "alutsista" mungkin relatif mudah diterapkan terhadap senapan atau tank. Namun, batas tersebut menjadi lebih sulit ketika objeknya adalah algoritma, *cloud computing*, sensor, *facial recognition*, drone komersial, *cyber tools*, atau perangkat lunak analisis data.

Jika dilihat dalam konteks yang lebih luas, perkembangan industri pertahanan Indonesia tidak lagi terbatas pada pemenuhan kebutuhan domestik saja, tetapi juga pada penguasaan teknologi, peningkatan kapasitas produksi dan perluasan pasar internasional, termasuk ke kawasan Afrika. Salah satu contohnya adalah hubungan PT Pindad dengan Rheinmetall Denel Munition (RDM), perusahaan industri pertahanan yang berbasis di Afrika Selatan dan merupakan perusahaan patungan antara Rheinmetall Waffe Munition Jerman dan Denel Afrika Selatan.⁴³ Kerja sama antara PT Pindad dan

⁴¹ Badan Teknologi Pertahanan Kementerian Pertahanan Republik Indonesia, "Design Requirement Rancang Bangun Weapon Integration System PTTA MALE Konsorsium," 7 Juli 2025, <https://www.kemhan.go.id/batekhan/2025/07/07/design-requirement-rancang-bangun-weapon-integration-system-ptta-male-konsorsium.html>.

⁴² Indonesia Defense, "Spesifikasi Drone Baru untuk Tugas Operasi Prajurit Marinir di Perbatasan," 17 April 2024, <https://indonesiadefense.com/spesifikasi-drone-baru-untuk-tugas-operasi-prajurit-marinir-di-perbatasan/>, diakses 8 September 2026.

⁴³ Rheinmetall menjelaskan bahwa RDM dimiliki bersama oleh Rheinmetall Waffe Munition GmbH (51 persen) dan Denel (Pty) Ltd., serta bergerak dalam produksi munisi kaliber menengah dan besar,

RDM, berlangsung setidaknya sejak tahun 2014 melalui pengembangan amunisi kaliber besar 6-155mm dengan skema yang mencakup penunjukan Pindad sebagai manufacturing hub RDM untuk Asia Pasifik, pertukaran tenaga ahli untuk transfer teknologi, serta rencana co-manufacturing di fasilitas Pindad di Turen, Malang. Pada 2024, hubungan tersebut diperkuat melalui Head of Agreement yang mencakup pasokan strategis propelan dan komponen amunisi kaliber 40 mm, transfer teknologi, alih fasilitas produksi (*transfer of manufacturing*), serta revitalisasi pabrik pengisian amunisi kaliber besar milik Pindad.⁴⁴

Pola tersebut bahkan semakin dalam ketika PT Dahana, BUMN yang juga tergabung dalam DEFEND ID, menandatangani MoU dengan RDM pada November 2025 untuk pembangunan fasilitas energetic material di Indonesia. Dalam skema tersebut, RDM berperan sebagai penyedia teknologi dan berkomitmen melakukan transfer teknologi, sementara fasilitas yang direncanakan dibangun di Energetic Material Center Dahana di Subang akan menghasilkan bahan energetik yang dibutuhkan untuk munisi kaliber besar dan isian hulu ledak, sekaligus memiliki fungsi dual-use untuk industri pertambangan.⁴⁵ Dalam perspektif kompleks industri-militer, hubungan Pindad–Dahana–RDM memperlihatkan terbentuknya jaringan industri pertahanan lintas negara yang menghubungkan BUMN, perusahaan pertahanan asing, transfer teknologi, fasilitas produksi, kepentingan diplomasi ekonomi, dan ekspansi pasar. Afrika sendiri semakin terlihat sebagai salah satu ruang ekspansi industri strategis Indonesia pada Indonesia Africa Forum 2024, pemerintah mencatat kerja sama PT Pindad dengan RDM di Afrika Selatan, sementara PT Dirgantara Indonesia juga memperluas hubungan bisnisnya dengan Republik Demokratik Kongo dan Senegal.⁴⁶

Setelah kami telusuri lebih jauh, hubungan kerja sama BUMN pertahanan Indonesia dengan Rheinmetall Denel Munition (RDM) menimbulkan kekhawatiran. Hubungan kerja sama ini perlu dibaca melalui rekam jejak rantai pasok global perusahaan tersebut. Investigasi Open Secrets pada 2020 mencatat bahwa RDM mengekspor munisi mortir 120 mm kepada Arab Saudi dan Uni Emirat Arab, dua negara utama dalam koalisi militer di Yaman. Investigasi tersebut juga menemukan bahwa fragmen amunisi yang ditemukan setelah serangan tahun 2018 di Hodeida yang menewaskan dan melukai warga sipil

sistem artileri dan mortir. Lihat Rheinmetall, “Rheinmetall Denel Munition (Pty) Ltd.,” <https://www.rheinmetall.com/en/company/subsidiaries/rheinmetall-denel-munition>.

⁴⁴PT Pindad (Persero), “Pindad Bersiap Menjadi Produsen Munisi Global,” 8 Agustus 2014, <https://pindad.com/pindad-bersiap-menjadi-produsen-munisi-global>.

⁴⁵ PT Dahana, “Dahana–RDM Sepakati Pembangunan Fasilitas *Energetic Material* di Indonesia,” 25 November 2025, <https://dahana.id/id/dahana-rdm-sepakati-pembangunan-fasilitas-energetic-material-di-indonesia/>.

⁴⁶ Kementerian Luar Negeri Republik Indonesia, “Indonesia dan Negara-Negara Afrika Tandatangani MoU Industri Strategis di IAF 2024,” 3 September 2024, <https://kemlu.go.id/berita/indonesia-dan-negara-negara-afrika-tandatangani-mou-industri-strategis-di-iaf-2024>.

memiliki sejumlah karakteristik yang serupa dengan mortir 120 mm produksi RDM. Temuan tersebut tidak dengan sendirinya membuktikan tanggung jawab hukum RDM atas serangan tersebut, tetapi memperlihatkan persoalan mendasar mengenai pengendalian pengguna akhir (end-user control) dan kemampuan perusahaan memastikan produk yang diekspor tidak digunakan dalam pelanggaran HAM atau hukum humaniter. Polemik tersebut bahkan mendorong pengetatan perizinan ekspor Afrika Selatan pada 2019, termasuk tuntutan inspeksi terhadap pengguna akhir yang sempat menghentikan izin ekspor ke Arab Saudi dan UEA.⁴⁷

Risiko serupa kembali muncul dalam konflik Sudan. Pada Juli 2025, Sunday Independent melaporkan tuduhan dari platform Sudanese Military Capabilities bahwa amunisi fosfor PHOS M8931 kaliber 40 mm yang diduga digunakan oleh Rapid Support Forces (RSF) dalam pertempuran di Khartoum dapat ditelusuri ke lini produksi American Rheinmetall Munitions dan RDM.⁴⁸ Persoalan yang lebih luas juga muncul pada jaringan korporasi Rheinmetall. Dalam komunikasi kepada Rheinmetall AG pada Mei 2024, sejumlah Pelapor Khusus dan ahli independen PBB menyatakan menerima informasi bahwa perusahaan tersebut terus memasok Israel dengan ratusan ribu amunisi tank presisi setelah 7 Oktober 2023, sementara menurut para ahli tersebut tidak terdapat informasi publik yang menunjukkan pelaksanaan enhanced human rights due diligence yang memadai untuk menilai risiko penggunaan senjata tersebut dalam konflik Gaza. Pada Juni 2024, para ahli PBB kemudian secara khusus memasukkan Rheinmetall AG di antara produsen senjata yang diminta menghentikan transfer ke Israel karena risiko keterlibatan dalam pelanggaran serius HAM dan hukum humaniter. Perlu dibedakan bahwa komunikasi PBB tersebut ditujukan kepada Rheinmetall AG, bukan RDM, meskipun RDM merupakan perusahaan patungan yang 51 persen sahamnya dimiliki Rheinmetall Waffe Munition, bagian dari Rheinmetall Group.⁴⁹

Rekam jejak ini membuat kerja sama Indonesia dengan RDM tidak dapat dilihat semata-mata sebagai persoalan alih teknologi dan kemandirian industri pertahanan. PT Pindad sebelumnya bahkan dirancang menjadi manufacturing hub RDM untuk kawasan Asia Pasifik, sementara pada 2025 PT Dahana kembali menandatangani kerja sama dengan RDM untuk membangun fasilitas energetic material di Indonesia. Ketika Indonesia semakin ditempatkan sebagai basis produksi sekaligus calon pemasok bagi pasar

⁴⁷ Zen Mathe dan Caryn Dolley, "Unaccountable 0004: Rheinmetall Denel Munition: Murder and Mayhem in Yemen," *Open Secrets*, 22 Januari 2020, <https://www.opensecrets.org.za/rheinmetall-denel-munition-murder-and-mayhem-in-yemen/>.

⁴⁸ Manuel Godsin, "Rheinmetall Denel Faces Scrutiny over Allegations of Arms Use in Sudan Conflict," *Sunday Independent/The Star*, 8 Juli 2025, <https://thestar.co.za/sundayindependent/news/2025-07-08-rheinmetall-denel-faces-scrutiny-over-allegations-of-arms-use-in-sudan-conflict/>.

⁴⁹ United Nations Human Rights Council, Special Procedures, "Communication to Rheinmetall AG," Ref. AL OTH 81/2024, 17 May 2024, 4, <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=29082>.

regional dan global, risiko HAM tidak lagi berhenti pada bagaimana teknologi digunakan oleh TNI, tetapi meluas ke siapa yang membeli produk yang dibuat di Indonesia, kepada siapa produk itu kemudian dialihkan, dan untuk operasi apa produk tersebut akhirnya digunakan.

Pada titik ini kompleks industri-militer kontemporer menjadi lebih kompleks daripada konfigurasi klasik yang dikritik Eisenhower pada 1961. Persoalannya tidak lagi berhenti pada hubungan antara militer, pemerintah, dan industri yang memperoleh keuntungan dari peningkatan anggaran serta produksi persenjataan di dalam satu negara. Industri pertahanan saat ini bekerja melalui rantai pasok transnasional, teknologi dikembangkan bersama perusahaan asing, komponen dan bahan baku diproduksi lintas negara, pengetahuan dialihkan melalui transfer teknologi, dan produk akhirnya dipasarkan kembali ke negara lain.

Ketika BUMN pertahanan Indonesia didorong untuk meningkatkan kapasitas produksi sekaligus memperluas pasar internasional, maka muncul risiko baru bahwa senjata, amunisi, bahan energetik, drone, perangkat pengawasan, maupun teknologi dual-use yang diproduksi atau dipasok dari Indonesia pada akhirnya digunakan oleh negara pembeli untuk tindakan yang melanggar HAM atau hukum humaniter internasional. Karena itu, kompleks industri-militer Indonesia lebih tepat dipahami bukan sebagai sistem yang sepenuhnya domestik, melainkan sebagai ekosistem transnasional yang berupaya membangun kapasitas produksi dalam negeri sekaligus menempatkan industri pertahanan Indonesia ke dalam pasar dan rantai pasok persenjataan global.

3. Bagaimana Dampak HAM dalam Penggunaan Teknologi Surveilans oleh Militer?

Manuel Castells dalam bukunya berjudul *The Rise of the Network Society* (2010), menegaskan bahwa realitas perkembangan teknologi telah membawa umat manusia hidup pada suatu era yang disebut di era digital. Castells menyamakan bahwa revolusi teknologi yang terjadi kini merupakan peristiwa sejarah yang sama besarnya dengan revolusi industri abad ke-18, sebab sama-sama memicu perubahan signifikan yang sifatnya pervasif, yakni penetrasi ke semua ranah aktivitas manusia. Inti transformasi yang kita alami dalam revolusi saat ini mengacu pada teknologi pemrosesan informasi dan komunikasi.⁵⁰

Dalam perspektif keamanan dan pertahanan, perkembangan teknologi khususnya dalam sektor pertahanan dan militer global telah menghadirkan konsep *The Internet of Military Things* (IoMT) atau *Battlespace Internet of Things* (BioT). Konsep tersebut menggambarkan penggunaan jaringan perangkat yang terhubung melalui internet, dan para aktor yang beroperasi di dalamnya. Australian Defence Force (ADF) bahkan telah berinvestasi dalam infrastruktur dan sistem komando dan kendali, komunikasi, komputer,

⁵⁰ Manuel Castells, *The Rise of the Network Society*, 2nd ed. (Chichester: Wiley-Blackwell, 2010), 29–30.

intelijen, pengawasan, dan pengintaian (C4ISR) untuk mengumpulkan, menganalisis, dan menyebarluaskan informasi.⁵¹

Lebih lanjut, transformasi teknologi tersebut juga mendapatkan adaptasi. Sebab telah menciptakan ruang baru dalam dinamika keamanan global yang dikenal sebagai ruang siber (*cyberspace*). Kelahiran ruang siber sebagai domain baru interaksi manusia dan negara juga telah merevolusi cara pengumpulan informasi dan praktik pengawasan dijalankan, sehingga ruang siber menjadi arena strategis baru bagi negara untuk melindungi kedaulatan digital, infrastruktur vital, dan kepentingan nasional.

Gambar 1 *How Cyberspace Is at the Leading Edge of Global Change*



Sumber: *The Diplomat*

Gambar di atas memperlihatkan ruang siber menghubungkan seluruh negara, tanpa perlu memandang sekat teritorial. Kondisi ini di satu sisi membawa kegamangan dalam aspek keamanan. Bahkan pada Konferensi Keamanan Munich (*Munich Security Conference/ MSC*) tahun 2016 yang dihadiri para pemimpin dunia, mereka menyerukan kesepakatan tentang norma-norma perilaku di dunia maya. Lebih dari 20 negara telah sepakat bahwa mereka tidak boleh saling menyerang infrastruktur penting satu sama lain selama masa damai. Norma-norma perusahaan masih dalam tahap awal, tetapi mungkin

⁵¹ Claire Withrington, "The Internet of Military Things," August 24, 2023, <https://cove.army.gov.au/article/internet-military-things>.

akan mencakup kebijakan untuk tidak menahan pembaruan keamanan dari pelanggan mana pun, di mana pun mereka berada.⁵²

Perkembangan teknologi informasi dan komunikasi secara fundamental telah mentransformasi cara lembaga intelijen beroperasi. Jika pada era Perang Dingin intelijen bergantung pada operasi fisik, infiltrasi, dan pengumpulan data lapangan, maka pada era digital, intelijen bergeser ke paradigma berbasis data (*data-driven intelligence*). Salah satu aspek paling menonjol dari perkembangan ini adalah meningkatnya penggunaan teknologi pengawasan sebagai instrumen utama dalam arsitektur pertahanan dan keamanan siber.

Dalam lanskap global, penguatan pengawasan terhadap individu, kelompok, atau negara yang menjadi perhatian telah semakin diawasi sejak 11 September 2001, atau peristiwa 9/11 di kota New York, Amerika Serikat. Bahkan CENTCOM (*United States Central Command*),⁵³ meminta bantuan RAND Corporation dalam mengembangkan instrumen untuk mengukur efektivitas operasi intelijen, pengawasan, dan pengintaian untuk mengevaluasi kinerja saat ini dan merencanakan, memengaruhi, dan menyediakan sumber daya untuk operasi di masa mendatang.⁵⁴

Militerisasi teknologi kini menjadi salah satu fokus utama dalam upaya memperkuat kapabilitas pertahanan berbagai negara. Departemen Pertahanan Amerika Serikat (*U.S. Department of Defense/DoD*) diperkirakan akan mengucurkan anggaran sekitar US\$384 miliar atau setara Rp6.424 triliun sebagai bagian dari strategi keamanan nasional yang bertujuan untuk memodernisasi seluruh matra militer serta meningkatkan investasi pada riset dan pengembangan pertahanan (R&D).⁵⁵

Menurut laporan *Investing in Defense Part III* yang dirilis oleh Visual Capitalist bekerja sama dengan Global X ETFs, total pengeluaran Amerika Serikat untuk teknologi pertahanan pada tahun fiskal 2026 diproyeksikan meningkat hingga 71 persen dibandingkan tahun 2020—dari US\$162,3 miliar menjadi US\$278 miliar. Lonjakan ini mencerminkan dorongan kuat militer AS untuk mengadopsi sistem pertahanan berteknologi tinggi yang mengintegrasikan kecerdasan buatan (AI), pengolahan data besar (*big data*), serta teknologi otonom dalam operasi darat, laut, dan udara.⁵⁶

Inggris juga sedang mempercepat upaya inovasi pertahanannya. Pemerintah Inggris telah berkomitmen untuk meningkatkan belanja pertahanan menjadi 2,5% dari PDB mulai

⁵² B. McConnell, "How Cyberspace Is at the Leading Edge of Global Change," *The Diplomat*, February 25, 2016, <https://thediplomat.com/2016/02/how-cyberspace-is-at-the-leading-edge-of-global-change>.

⁵³ Merupakan komando militer Amerika Serikat yang bertanggung jawab untuk wilayah yang mencakup sebagian besar Timur Tengah, Asia Tengah, dan Afrika. Misi utamanya adalah mempertahankan dan mempromosikan kepentingan AS di wilayah tersebut, yang mencakup operasi militer, bantuan kemanusiaan, serta latihan bersama dengan negara-negara mitra lihat U.S. Central Command, "About Us," <https://www.centcom.mil/ABOUT-US/>.

⁵⁴ David Luckey et al., *Measuring Intelligence, Surveillance, and Reconnaissance Effectiveness at the United States Central Command* (Santa Monica, CA: RAND Corporation, 2021).

⁵⁵ Elvan Widyatama, "Gila-Gilaan! AS Habiskan Rp6.000 T Buat Teknologi Perang Masa Depan," *CNBC Indonesia*, November 13, 2025, <https://www.cnbcindonesia.com/research/20251112105824-128-684492/gila-gilaan-as-habiskan-rp6000-t-buat-teknologi-perang-masa-depan>.

⁵⁶ Widyatama, "Gila-Gilaan! AS Habiskan Rp6.000 T Buat Teknologi Perang Masa Depan."

tahun 2027, dengan aspirasi jangka panjang sebesar 3,5% dari PDB untuk belanja pertahanan “inti” dan 1,5% untuk “ketahanan dan keamanan” pada tahun 2035, yang berarti total 5% dari pendapatan nasional untuk keamanan nasional. Peningkatan signifikan ini akan mendorong investasi di bidang-bidang seperti teknologi drone, sistem senjata laser, senjata jarak jauh, dan amunisi canggih.⁵⁷

Dalam konteks Indonesia, adaptasi penguatan pertahanan dengan lokus ruang siber juga terlihat. Dalam kerangka UU No. 3 Tahun 2002 tentang Pertahanan Negara, ruang siber belum termasuk perhatian. Sebab dalam penjelasan UU *a quo*, lingkup permasalahan yang berkaitan dengan globalisasi hanya meliputi terorisme, imigran gelap, bahaya narkoba, pencurian kekayaan alam, bajak laut, dan kerusakan lingkungan. Namun, melalui UU No. 23 Tahun 2019 tentang Pengelolaan Sumber Daya Nasional Untuk Pertahanan Negara, pada Pasal 4 ayat (2) dan (3) telah dijelaskan bahwa serangan siber telah disebutkan sebagai salah satu bentuk ancaman.

Dalam konteks pertahanan, terutama ISR (*Intelligence, Surveillance, and Reconnaissance*), perlu dipahami bahwa keberadaannya memiliki peran signifikan bagi militer dalam upayanya menjaga pertahanan negara.⁵⁸ Kerja-kerja ISR yang meliputi pengumpulan, analisis, dan penyebaran informasi, membantu pengambilan keputusan dalam operasi pertahanan, keamanan, dan respons krisis, sehingga membuat militer mampu mendeteksi ancaman dan memberikan respons secara efektif berbagai skenario yang berkembang.⁵⁹ Namun demikian, penguatan ruang siber dan penggunaan teknologi surveilans membangun suatu perdebatan etis tentang implikasi jangkauan intelijen keamanan negara yang berfokus pada upaya menyeimbangkan hak, kebebasan, dan privasi individu dengan keamanan negara.⁶⁰

Diskursus ini muncul karena perkembangan teknologi yang mulanya diorientasikan untuk penguatan keamanan nasional sekalipun juga memiliki potensi penyalahgunaan. Kekuasaan, informasi, dan kontrol berkelindan dalam ruang siber tersebut. Sebab teknologi terkait digunakan penguasa sebagai alat pengawasan yang invasif bagi ruang-ruang privasi warga, sehingga mengakibatkan berbagai bentuk pelanggaran terhadap Hak Asasi Manusia.

⁵⁷ Timo Stellpflug, “The Resurgence of European and UK Defence Tech: Markets, Technology, and Investment,” *Taylor Wessing*, July 31, 2025, <https://www.taylorwessing.com/en/interface/2025/defence-tech/the-resurgence-of-european-and-uk-defence-tech>.

⁵⁸ ISR terdiri dari 3 komponen yang saling melengkapi. Intelijen sebagai penganggalan informasi yang telah diproses dan dianalisis. Surveilans sebagai pemantauan berkelanjutan terhadap suatu area, individu, atau aktivitas dari waktu ke waktu. Lalu Reconnaissance atau pengintaian yang bertujuan untuk mengumpulkan informasi spesifik tentang suatu area, objek, atau ancaman tertentu, seringkali dalam kondisi yang sensitif terhadap waktu. Lebih lanjut, misi pengintaian berperan penting dalam memverifikasi intelijen lainnya. Lihat Elistair, “Intelligence, Surveillance, and Reconnaissance (ISR),” <https://elistair.com/glossary/intelligence-surveillance-reconnaissance/>.

⁵⁹ Elistair, “Intelligence, Surveillance, and Reconnaissance (ISR).”

⁶⁰ Adam Henschke, *Ethics in an Age of Surveillance: Personal Information and Virtual Identities* (Cambridge: Cambridge University Press, 2017); Laura Muir, “Control Space?: Cinematic Representations of Surveillance Space between Discipline and Control,” *Urban Surveillance* 9, no. 3 (2012): 263–279.

Gambar 2 *The Use of Black Faces in Facial Recognition Systems*



Sumber: epic.org

Melalui gambar di atas, perlu diketahui bahwa banyak perusahaan teknologi Tiongkok terus mengeksport teknologi pengenalan wajah mereka ke pasar Afrika sambil mendukung praktik pengawasan domestik yang mencakup deteksi etnis Uyghur dan minoritas etnis lainnya. Teknologi pengenalan wajah, yang dulunya dianggap sebagai solusi potensial untuk tantangan sosial seperti kejahatan, kini banyak dikritik karena bias rasial dan risiko yang ditimbulkan teknologi tersebut terhadap privasi dan kebebasan sipil.⁶¹

Peron, AE dos R., Almstadter Mattar de Magalhães, D., & Caetano, GF (2025), memperkenalkan konsep tekno-otoritarianisme (*techno-authoritarianism*) sebagai titik temu atau hubungan antara otoritarianisme dan teknologi. Konsep ini diadopsi mengingat semakin eratnya kaitan antara otoritarianisme dan beragam perangkat teknologi yang dapat menyebabkan keretakan demokrasi. Istilah ini juga dapat menggambarkan dan memahami penggunaan sumber daya teknologi secara ekstensif yang merongrong prinsip-prinsip demokrasi dan hak-hak asasi.⁶²

Sebab pemerintah di seluruh dunia pada dasarnya telah menggunakan sistem pengawasan berbasis AI yang disamarkan sebagai metode "cerdas" untuk pengendalian

⁶¹ B. Jili, "The Rise of Chinese Surveillance Technology in Africa," Electronic Privacy Information Center (EPIC), May 31, 2022, <https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa/>.

⁶² A. E. dos R. Peron, D. Almstadter Mattar de Magalhães, dan G. F. Caetano, "Beyond Digital Repression: Techno-Authoritarianism in Radical Right Governments," *Cogent Social Sciences* 11, no. 1 (2025), <https://doi.org/10.1080/23311886.2025.2528457>.

kejahatan. Namun, penggunaannya yang selaras dengan disrupsi institusional dan demokrasi, justru menciptakan bentuk-bentuk represi terhadap mereka yang menentang pemerintahan tersebut.⁶³

3.1. Pelanggaran terhadap Kebebasan Berpendapat, Berekspresi, dan Berkumpul

3.1.1. Jaminan atas Kebebasan Berpendapat, Berekspresi, dan Berkumpul

Konstitusi melalui Pasal 28 E ayat (3) UUD tahun 1945 yang menyatakan “Setiap orang berhak atas kebebasan berserikat, berkumpul, dan mengeluarkan pendapat”. Jaminan tersebut dirinci dalam UU No. 9 Tahun 1998 tentang Kemerdekaan Menyampaikan Pendapat di Muka Umum. Pada konsiderans huruf a dan b, *UU a quo* menegaskan bahwa kemerdekaan menyampaikan pendapat di muka umum adalah hak asasi manusia yang dijamin oleh Undang-Undang Dasar 1945 dan Deklarasi Universal Hak-hak Asasi Manusia, kemudian kemerdekaan setiap warga negara untuk menyampaikan pendapat di muka umum merupakan perwujudan demokrasi dalam tatanan kehidupan bermasyarakat, berbangsa, dan bernegara.

Selain itu, sejumlah norma *UU a quo* semakin menegaskan jaminan kebebasan berpendapat bagi setiap warga negara, serta menjadi bagian dari hak demokrasi. Pasal 2 ayat (1) menyatakan bahwa setiap warga negara, secara perorangan atau kelompok menyampaikan pendapat sebagai perwujudan hak dan tanggung jawab berdemokrasi dalam kehidupan bermasyarakat, berbangsa, dan bernegara. Lalu pada Pasal 5 juga ditegaskan bahwa warga negara yang menyampaikan pendapat di muka umum berhak untuk mengeluarkan pikiran secara bebas dan memperoleh perlindungan hukum.

Meskipun kebebasan menyampaikan pendapat secara hukum tergolong sebagai *derogable right*—yakni hak yang dapat dikenai pembatasan dalam kondisi tertentu—namun sifat derogabel tersebut tidak serta-merta mengurangi makna fundamentalnya dalam tatanan demokrasi. Dalam konteks hukum nasional, pembatasan tersebut diatur antara lain dalam Pasal 9 ayat (2) Undang-Undang Nomor 9 Tahun 1998, yang menetapkan bahwa penyampaian pendapat tidak dapat dilakukan di tempat-tempat tertentu demi menjaga ketertiban umum, keselamatan, dan kepentingan strategis negara. Pembatasan ini, secara teori, merupakan bentuk *regulasi prosedural* yang bertujuan mengharmoniskan penggunaan hak dengan kepentingan publik yang lebih luas.

Namun demikian, prinsip dasarnya tetap harus ditegaskan: hak untuk menyampaikan pendapat di muka umum adalah hak konstitusional warga negara yang dilindungi, bukan anugerah negara yang dapat dicabut secara sewenang-wenang. Dalam kerangka hukum hak asasi manusia, fakta bahwa suatu hak dapat dibatasi tidak berarti negara memiliki kebebasan absolut untuk mengintervensinya. Pembatasan hanya sah apabila memenuhi prinsip legalitas, proporsionalitas, dan tujuan yang sah (*legitimate aim*) sebagaimana ditegaskan dalam Pasal 19 ayat (3) *International Covenant on Civil and Political Rights* (ICCPR), yang telah diratifikasi Indonesia.

⁶³ Peron, Magalhães, dan Caetano, “Beyond Digital Repression.”

Dengan kata lain, meskipun hak untuk menyampaikan pendapat dapat diatur, ia tidak dapat ditiadakan. Hak ini tetap melekat pada setiap warga negara sebagai *core democratic right* yang menjadi dasar keberlangsungan pemerintahan yang terbuka, akuntabel, dan responsif. Hal ini terlihat melalui konstruksi Pasal 7 UU No. 9 Tahun 1998 yang menegaskan kewajiban dan tanggung jawab aparat pemerintah terhadap pelaksanaan penyampaian pendapat di muka umum oleh warga negara, yakni: (a) melindungi hak asasi manusia; (b) menghargai asas legalitas; (c) menghargai prinsip praduga tidak bersalah; dan (d) menyelenggarakan pengamanan.

Secara lebih prinsipil, UU No. 39 Tahun 1999 tentang Hak Asasi Manusia memberikan fondasi normatif yang tegas mengenai posisi hak asasi manusia dalam sistem hukum Indonesia. Pada Pasal 2, undang-undang ini menyatakan bahwa negara *mengakui dan menjunjung tinggi hak asasi manusia dan kebebasan dasar manusia sebagai hak yang secara kodrati melekat pada dan tidak terpisahkan dari manusia*. Rumusan ini menunjukkan bahwa negara tidak memiliki otoritas untuk “memberikan” atau “menghapus” hak tersebut, karena hak asasi bukan berasal dari negara, melainkan dari kodrat manusia itu sendiri. Negara hanya berkewajiban melindungi, menghormati, dan menegakkan hak-hak tersebut demi martabat kemanusiaan, kesejahteraan, kebahagiaan, kecerdasan, dan keadilan bagi seluruh warga.

Jika negara gagal memenuhi prinsip-prinsip tersebut, maka pembatasan berubah menjadi pelanggaran, dan negara justru bertindak bertentangan dengan mandat konstitusional dan hukum HAM nasional. Lebih jauh, dalam konteks kontemporer yang ditandai oleh meningkatnya militerisasi ruang siber, prinsip-prinsip dalam Pasal 2 menjadi semakin penting. Penggunaan berbagai teknologi pemantauan digital, mekanisme pengawasan siber, dan perluasan kewenangan aparat keamanan sering kali dilakukan atas nama stabilitas keamanan nasional. Namun tanpa pengawasan yang ketat, praktik ini mudah berubah menjadi bentuk kontrol yang mengekang kebebasan berpendapat dan mengikis privasi warga negara.

3.1.2. Tekno-Otoritarianisme: Ketika Teknologi Digunakan sebagai Instrumen yang Melanggar HAM

Secara paradigmatik, militerisasi dalam pengelolaan ruang siber merupakan manifestasi dari konsep tekno-otoritarianisme yang menegaskan tentang pengendalian dan pengawasan ruang siber dengan dalih pertahanan-keamanan, atau stabilitas. Ketika negara mengadopsi logika militeristik dalam pengelolaan ruang siber, terutama melalui pendekatan pertahanan dan keamanan yang represif, maka ruang tersebut berpotensi kehilangan karakter demokratisnya. Transformasi ruang digital menjadi domain yang diawasi, dikendalikan, dan diproteksi dengan cara-cara militeristik yang tidak menempatkan prinsip-prinsip hak asasi manusia sebagai hal yang fundamental. Akibatnya, teknologi digital telah memberi pemerintahan otoriter alat baru untuk mengendalikan, membungkam, dan menghukum perbedaan pendapat lintas batas. Teknologi digital memungkinkan rezim untuk memantau dan merespons aktivitas politik warga negaranya dalam wilayah yurisdiksinya, tetapi hingga komunitas diaspora di luar

negeri. Dengan demikian, teknologi digital telah menjadi komponen penting dalam perangkat represi transnasional.⁶⁴

Gambar 3 *Digital Authoritarianism in the Middle East*



Sumber: *thesecuritydistillery.org*

Tekno-otoritarianisme juga menjadi fenomena di Timur Tengah, meski dengan menggunakan istilah otoritarianisme digital.⁶⁵ Selama sepuluh tahun terakhir, pemerintah di sejumlah negara Timur Tengah telah menggunakan teknologi informasi dan komunikasi digital sebagai alat untuk memperkuat kontrol atas warga negara mereka. Mengambil inspirasi dari model yang diberikan Tiongkok, Rusia, dan Israel, kemudian pemerintah Timur Tengah telah menerapkan kebijakan dan strategi yang bertujuan untuk sensor, penipuan digital, dan pengawasan massal yang memperburuk catatan HAM di kawasan tersebut.⁶⁶

Misalnya di Mesir, seiring meningkatnya penggunaan internet di Mesir, upaya pemerintah untuk mengendalikan ruang digital dan memberlakukan pengawasan yang lebih ketat

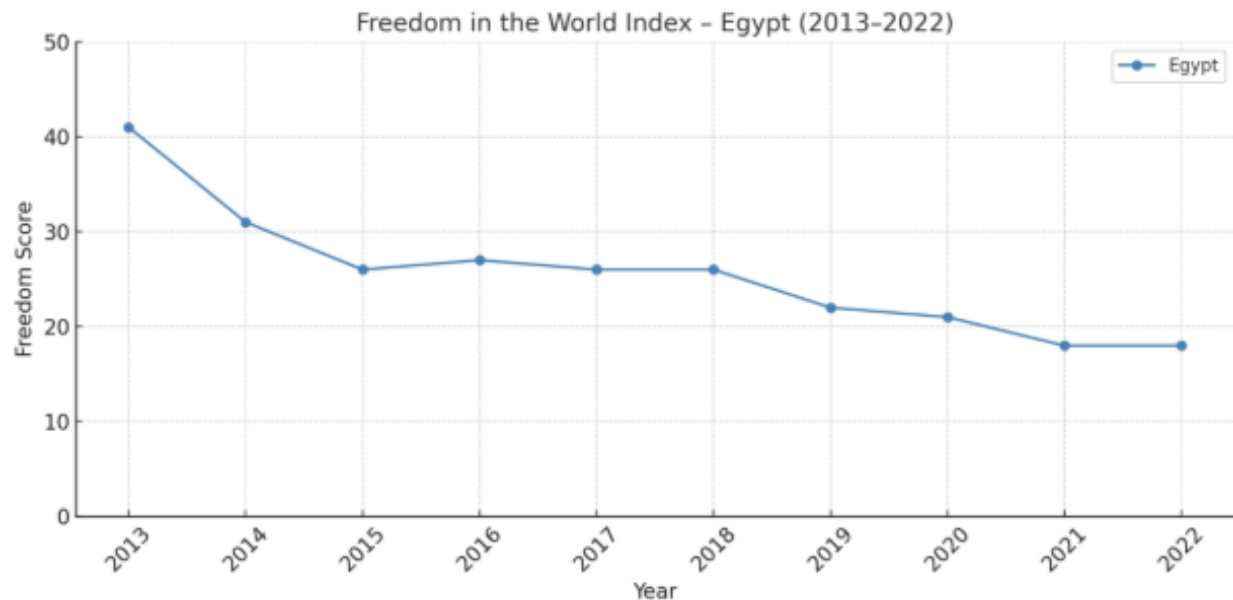
⁶⁴ Marcus Michaelsen, *The Digital Transnational Repression Toolkit, and Its Silencing Effects* (Freedom House, 2020), <https://freedomhouse.org/report/special-report/2020/digital-transnational-repression-toolkit-and-its-silencing-effects>.

⁶⁵ Brookings Institution mendefinisikan otoritarianisme digital sebagai “penggunaan teknologi informasi dan komunikasi digital oleh negara-negara otoriter dan otokratis untuk memantau, memanipulasi, menindas, dan mengendalikan penduduk.” Lihat Alina Polyakova and Chris Meserole, *Exporting Digital Authoritarianism: The Russian and Chinese Models* (Washington, DC: Brookings Institution, 2019).

⁶⁶ Giorgia Piovesan, “Digital Authoritarianism in the Middle East,” *The Security Distillery*, April 19, 2023, <https://thesecuritydistillery.org/all-articles/digital-authoritarianism-in-the-middle-east>.

terhadap masyarakat juga semakin meningkat. Situs web Human Rights Watch diblokir oleh otoritas Mesir hanya sehari setelah organisasi tersebut merilis laporan tentang penyiksaan sistematis di penjara-penjara negara tersebut.⁶⁷ Indeks *Freedom House* menunjukkan bahwa rata-rata kebebasan internet telah menurun sekitar 40% di Mesir.

Gambar 4



Sumber: *Freedom House*, 2022

Indeks yang disusun *Freedom House* menunjukkan bahwa Mesir telah mengalami penurunan dalam kebebasan berekspresi dan berkeyakinan, hak berorganisasi dan berserikat, supremasi hukum, serta otonomi pribadi dan hak-hak individu.⁶⁸ Pemerintah Mesir berfokus pada empat domain: kerangka hukum yang restriktif, sensor internet, pengawasan perkotaan, dan SDIO (*Social Media Information Organizations*). Dengan memanfaatkan keempat domain ini, pemerintah Mesir telah membangun sistem otoritarianisme digital yang komprehensif. Sistem ini tidak hanya memperkuat cengkraman kekuasaan, tetapi juga berfungsi sebagai cetak biru bagi rezim otoriter lain yang berupaya memanfaatkan teknologi digital untuk menekan perbedaan pendapat dan mempertahankan kendali.⁶⁹

⁶⁷ Al Jazeera, "Egypt Blocks Human Rights Watch Website," September 8, 2017, <https://www.aljazeera.com/news/2017/9/8/egypt-blocks-human-rights-watch-website>.

⁶⁸ Freedom House, "Egypt," *Freedom on the Net* 2022, 2022, <https://freedomhouse.org/country/egypt/freedom-net/2022>.

⁶⁹ Ihsan Yilmaz, Ali Mamouri, Shahram Akbarzadeh, and Muhammad Omer, *Authoritarian Diffusion in the Cyberspace: How Egypt Learns, Emulates, and Cooperates in Digital Authoritarianism* (Brussels: European Center for Populism Studies, 2025), May 9, 2025, <https://doi.org/10.55271/rp0097>.

Dalam konteks kerangka hukum yang restriktif, ketentuan di Mesir berupa:

1. Undang-Undang yang mewajibkan penyedia layanan internet untuk membangun sistem pemantauan dan perekaman lalu lintas secara *real-time* di jaringan mereka. Hal ini memungkinkan pengawasan terus-menerus terhadap aktivitas daring;
2. Kerangka hukum yang menghukum kebebasan berbicara daring dengan dalih melindungi identitas nasional, budaya, dan mencegah pencemaran nama baik. Hal ini seringkali mengakibatkan penindasan terhadap pendapat yang berbeda dan kebebasan berekspresi;
3. Pembatasan VPN, yang mengikuti jejak negara-negara seperti Tiongkok dan Rusia untuk melarang atau membatasi penggunaan Jaringan Pribadi Virtual (VPN). Meskipun VPN secara teknis legal di Mesir, banyak server dan situs web VPN diblokir, sehingga menghambat penggunaan praktisnya; dan
4. Kontrol terhadap perusahaan media sosial dengan berbagai metode, seperti mengancam perusahaan terkait dengan pembatasan bandwidth dan larangan langsung jika mereka gagal mematuhi permintaan pemerintah.⁷⁰

Bahkan di Mesir juga terdapat UU Kejahatan Siber tahun 2018 yang memperlakukan semua akun media sosial dengan lebih dari 5.000 pengikut sebagai *outlet media*, sehingga memenuhi syarat untuk disensor.⁷¹ Undang-Undang tersebut juga mewajibkan penyedia layanan internet untuk membangun sistem yang memungkinkan pemantauan dan perekaman lalu lintas secara *real-time* di jaringan mereka.⁷² Undang-Undang kejahatan siber mengkriminalisasi segala bentuk ucapan yang bertentangan dengan keamanan nasional, serta mengizinkan penggeledahan perangkat pribadi warga negara dan akun media sosial dapat diblokir tanpa otorisasi pengadilan, dengan alasan menyebarkan informasi palsu atau menghasut kegiatan yang melanggar hukum.⁷³

Sementara dalam konteks Indonesia, otoritarianisme digital menjadi manifestasi militerisasi ruang siber yang sedang terjadi. Menjelang tiga dekade setelah Reformasi 1998, masyarakat sipil Indonesia nyatanya masih menghadapi tantangan serius: semakin menguatnya otoritarianisme, represi terhadap kebebasan berekspresi, serta penyalahgunaan teknologi untuk mengendalikan narasi dan meminggirkan suara-suara kritis. Represi tersebut memicu berbagai bentuk pelanggaran terhadap kebebasan berpendapat, berekspresi, dan berserikat.⁷⁴

⁷⁰ Marwa Fatafta, "Egypt's New Data Protection Law: Data Protection or Data Control?" *Access Now*, September 24, 2020, <https://www.accessnow.org/egypts-new-data-protection-law-data-protection-or-data-control/>.

⁷¹ Reporters Without Borders (RSF), "Egypt's New Cybercrime Law Legalizes Internet Censorship," August 21, 2018, <https://rsf.org/en/egypt-s-new-cybercrime-law-legalizes-internet-censorship>.

⁷² Privacy International, "State of Privacy: Egypt," January 26, 2019, <https://www.privacyinternational.org/state-privacy/1001/state-privacy-egypt>.

⁷³ Ihsan Yilmaz, Ali Mamouri, Shahram Akbarzadeh, and Muhammad Omer, "Authoritarian Diffusion in the Cyberspace: How Egypt Learns, Emulates, and Cooperates in Digital Authoritarianism," *European Center for Populism Studies*, May 9, 2025, <https://www.populismstudies.org/authoritarian-diffusion-in-the-cyberspace-how-egypt-learns-emulates-and-cooperates-in-digital-authoritarianism/>.

⁷⁴ Lihat LP3ES, "Membangun Resiliensi Masyarakat Sipil Setelah 27 Tahun Reformasi," May 22, 2025, <https://www.lp3es.or.id/2025/05/22/membangun-resiliensi-masyarakat-sipil-setelah-27-tahun-reformasi/>.

Gambar 5 Karikatur Pengekangan Kebebasan Berpendapat dan Berekspresi



Sumber: *Radioidola*

Kondisi otoritarianisme digital di Indonesia tercermin dalam lima tahun terakhir, 2020–2024, ketika skor kebebasan internet menurut Freedom House cenderung stagnan dan konsisten berada dalam kategori *Partly Free* (bebas sebagian) yang menunjukkan bahwa suatu negara, dalam hal ini Indonesia, memiliki akses internet yang meningkat, namun masih menghadapi tantangan signifikan terhadap kebebasan online, termasuk pembatasan, sensor, dan serangan terhadap pengguna.⁷⁵

⁷⁵ Skor didasarkan pada skala 0 (paling tidak bebas) hingga 100 (paling bebas). Kategori ini mencakup skor: di bawah 35 adalah “Not Free” (Tidak Bebas), lalu skor 35-69 adalah “Partly Free” (Bebas Sebagian), dan skor 70-100 adalah “Free” (Bebas).

Tabel 1. Skor Kebebasan Internet di Indonesia Tahun 2020-2024

No	Tahun	Skor	Sorotan Isu
1	2020	49/100	Meningkatnya disinformasi dan propaganda pro-pemerintah, serta serangan teknis terhadap aktivis, jurnalis, dan kelompok masyarakat sipil. Pemerintah juga kembali membatasi akses internet, termasuk pemutusan konektivitas di Papua dan Papua Barat pada Agustus–September 2019 di tengah gelombang protes. Meski dinyatakan melanggar hukum oleh pengadilan, praktik tersebut menunjukkan kecenderungan penggunaan kontrol digital sebagai respons politik. Di saat yang sama, kriminalisasi dan pelecehan terhadap kritik daring terus mempersempit ruang kebebasan berekspresi di ranah digital. ⁷⁶
2	2021	48/100	Munculnya regulasi baru yang mewajibkan penghapusan konten dan pendaftaran bagi perusahaan teknologi, yang berdampak pada kebebasan berekspresi daring. Akses internet di Papua kembali mengalami gangguan, termasuk pada momen-momen sensitif terkait isu kemerdekaan. Di saat yang sama, kritikus pemerintah, jurnalis, dan pengguna internet biasa terus menghadapi tuntutan pidana dan pelecehan atas aktivitas daring mereka. Serangan teknis terhadap jurnalis, media, dan lembaga think tank juga meningkat seiring dengan peliputan isu-isu kritis. ⁷⁷
3	2022	49/100	Akses internet di Papua kembali mengalami gangguan, termasuk pada momen yang berkaitan dengan isu kemerdekaan Papua. Di ruang digital, kritik terhadap pemerintah masih dibalas dengan tuntutan pidana, pelecehan, serta peningkatan serangan teknis terhadap jurnalis, media, dan lembaga think tank. Di luar periode pelaporan, otoritas juga memperketat kewajiban registrasi dan penghapusan konten bagi perusahaan teknologi, yang sempat berujung pada pemblokiran sementara sejumlah platform. ⁷⁸

⁷⁶ Freedom House, “Indonesia: Freedom on the Net 2020 Country Report,” 2020, <https://freedomhouse.org/country/indonesia/freedom-net/2020> .

⁷⁷ Freedom House, “Indonesia: Freedom on the Net 2021 Country Report,” 2021, <https://freedomhouse.org/country/indonesia/freedom-net/2021> .

⁷⁸ Freedom House, “Indonesia: Freedom on the Net 2022 Country Report,” 2022, <https://freedomhouse.org/country/indonesia/freedom-net/2022> .

4	2023	47/100	Kondisi kebebasan internet di Indonesia memburuk, terutama akibat penerapan Peraturan Menteri Nomor 5 Tahun 2020 yang memperluas rezim moderasi konten dan mengancam kebebasan berekspresi serta privasi pengguna. Pada Juni 2022, pemerintah memblokir sementara sejumlah platform yang tidak memenuhi kewajiban pendaftaran. Di saat yang sama, kritikus pemerintah, jurnalis, dan pengguna internet terus menghadapi kriminalisasi, kekerasan, dan pelecehan daring, sementara gangguan akses internet di Papua masih berulang. ⁷⁹
5	2024	49/100	Kampanye kebencian daring terhadap pengungsi Rohingya dan penyebaran disinformasi meningkat tajam menjelang Pemilu Februari 2024. Pada saat yang sama, pengkritik pemerintah, jurnalis, dan pengguna internet terus menghadapi tuntutan pidana, kekerasan, dan pelecehan sebagai balasan atas aktivitas daring mereka. Elite politik dan ekonomi, termasuk aktor yang terkait dengan partai besar dan militer, juga memanipulasi opini publik di media sosial melalui penggunaan buzzer berbayar. ⁸⁰

Sumber: *Freedom House 2020-2024*

Rangkaian temuan *Freedom House* sejak 2020 hingga 2024 menunjukkan bahwa kemunduran kebebasan internet di Indonesia bukanlah peristiwa insidental, melainkan bagian dari trayektori otoritarianisme digital yang mengkonsolidasi diri secara bertahap. Negara tidak sepenuhnya menutup akses digital, tetapi secara sistematis membangun perangkat hukum, teknis, dan politik untuk mengendalikan arus informasi, membentuk opini publik, dan membatasi ekspresi kritis, terutama pada momen-momen sensitif.

Praktik gangguan dan pembatasan akses internet, khususnya di Papua, menjadi pola berulang dari tahun ke tahun. Pemutusan akses bukan respons darurat semata, melainkan strategi pengendalian informasi berbasis wilayah. Tekanan terhadap aktor kritis—jurnalis, aktivis, peneliti, dan pengguna internet biasa—menjadi elemen konsisten sepanjang periode 2020–2024. Kriminalisasi, pelecehan daring, serangan teknis, hingga kekerasan fisik berfungsi menciptakan efek gentar (*chilling effect*), yang membuat warga melakukan sensor diri. Bahkan Menjelang Pemilu 2024, dimensi lain dari otoritarianisme

⁷⁹ Freedom House, “Indonesia: Freedom on the Net 2023 Country Report,” 2023, <https://freedomhouse.org/country/indonesia/freedom-net/2023>.

⁸⁰ Freedom House, “Indonesia: Freedom on the Net 2024 Country Report,” 2024, <https://freedomhouse.org/country/indonesia/freedom-net/2024>.

digital semakin terlihat, yakni manipulasi wacana melalui disinformasi terorganisir dan buzzer berbayar.

Dampak otoritarianisme digital di Indonesia juga terlihat melalui survei yang dilakukan LP3ES terhadap 1.658 organisasi masyarakat sipil (OMS). Survei tersebut mengungkapkan bahwa 31% masyarakat sipil mengalami ancaman dan represi digital dalam berbagai bentuk, seperti peretasan, *phising*, dan intimidasi. Menariknya, survei tersebut menemukan dua pola yang mengemuka, yakni (1) prevalensi ancaman yang tinggi di wilayah urban dan industrial seperti di Jakarta, Jawa Barat, dan Jawa Tengah, serta (2) serangan digital yang muncul di wilayah yang kaya mineral seperti Kalimantan Timur, Sulawesi Tengah, serta Maluku.⁸¹

Perkembangan teknologi justru hadir dengan wajah gelap dan dijalankan kekuasaan. Terdapat tiga pola utama penggunaan represi digital di Indonesia. Dua di antaranya bahkan rentan atau berpotensi melibatkan aktor-aktor keamanan. Pola-pola tersebut, yakni:

1. Teror siber dengan segala bentuknya mulai dari peretasan, pengambilalihan akun media sosial, pengintaian kegiatan di internet, hingga telepon terus-menerus dengan berbagai nomor tidak dikenal;
2. Kriminalisasi menggunakan pasal karet yang ada dalam peraturan perundangan terkait dengan internet, dalam hal ini salah satu perundangan yang sering digunakan adalah UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), terutama Pasal 27 Ayat 3 tentang pencemaran nama baik dan Pasal 28 Ayat 2 tentang ujaran kebencian.⁸²

Laporan Amnesty International juga menyebutkan bahwa penyalahgunaan teknologi pengawasan, serta penggunaan teknologi yang tidak sejalan dengan HAM, seperti *spyware* yang sangat invasif, merupakan beberapa dari sekian banyak taktik yang digunakan di seluruh dunia untuk mempersempit ruang publik. Di saat yang sama, pembela HAM dan aktivis justru berulang kali menghadapi represi daring di Indonesia, salah satunya melalui UU No. 1 Tahun 2024 tentang Perubahan Kedua atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.⁸³ Kondisi ini terlihat melalui data Amnesty International Indonesia yang mencatat terdapat 527 kasus pelanggaran kebebasan berekspresi berbasis UU ITE kepada sedikitnya 560 warga terjadi sejak 2019 hingga 2024. Dari jumlah tersebut, terdapat 421 kasus dengan 449 korban telah mendapat vonis pengadilan.⁸⁴

⁸¹ LP3ES, "Membangun Resiliensi Masyarakat Sipil Setelah 27 Tahun Reformasi."

⁸² Wijayanto, "Masyarakat Sipil dan Represi Digital," *Kompas*, 10 Juni 2025, <https://www.kompas.id/artikel/melindungi-masyarakat-sipil-dari-represi-digital-2>.

⁸³ Amnesty International, "Unravelling a Murky Network of Spyware Exports to Indonesia," 17 Mei 2024, <https://www.amnesty.org/en/latest/news/2024/05/unravelling-a-murky-network-of-spyware-exports-to-indonesia/>.

⁸⁴ Amnesty International Indonesia, "'Arus Balik' Hak Asasi Manusia di 100 Hari Pemerintahan Baru," 21 Januari 2025, <https://www.amnesty.id/kabar-terbaru/siaran-pers/arus-balik-hak-asasi-manusia-di-100-hari-pemerintahan-baru/01/2025/>.

Selain itu, tidak kalah penting melihat problematika ini dalam kerangka pengarusutamaan gender. Perempuan dan kelompok berbasis gender lainnya kerap mengalami kerentanan berlapis akibat praktik pengawasan yang semakin intensif dan tidak transparan. Pengawasan digital juga berpotensi memperbesar risiko kekerasan berbasis gender daring (*online gender-based violence*), seperti doxing, pelecehan digital, intimidasi, dan kriminalisasi berbasis ekspresi, yang berdampak pada pembatasan ruang partisipasi perempuan di ruang publik dan politik.

Teknologi biometrik, termasuk pengenalan wajah, pemindaian sidik jari, dan deteksi iris, semakin terintegrasi ke dalam sistem pengawasan, sehingga menimbulkan kekhawatiran kritis tentang privasi dan kesetaraan. Gender memainkan peran penting dalam penerapan dan dampak teknologi ini, karena bias yang tertanam dalam sistem biometrik secara tidak proporsional memengaruhi perempuan, individu non-biner, dan komunitas yang terpinggirkan. Persimpangan antara gender dan pengawasan mengungkapkan ketidaksetaraan struktural, di mana bias algoritmik dalam identifikasi biometrik sering kali salah mengidentifikasi atau mengecualikan kelompok tertentu, memperkuat kesenjangan sosial yang ada.⁸⁵

Baru-baru ini, persoalan tersebut juga kental terlihat ketika patroli siber yang dilakukan Satuan Siber TNI ketika demonstrasi Agustus 2025 lalu yang menemukan sejumlah dugaan tindak pidana. Salah satu hasil dari patroli siber tersebut berupa kedatangan Komandan Satuan Siber (Dansat Siber) Mabes TNI dan sejumlah perwira tinggi TNI ke Polda Metro Jaya untuk konsultasi dugaan tindak pidana yang dilakukan CEO Malaka Project Ferry Irwandi.

Sementara UU No. 3 Tahun 2025 tentang TNI, pada Pasal 7 ayat (2) huruf b telah memandatkan salah satu tugas TNI dalam Operasi Militer Selain Perang (OMSP) berkaitan dengan bidang siber, yakni membantu dalam upaya ancaman pertahanan siber, tetapi pada bagian penjelasan ketentuan terkait, telah ditegaskan bahwa konteks ancaman siber yang dimaksud adalah pada sektor pertahanan (*cyber defense*), bukan yang berkaitan dengan penegakan hukum. Langkah ini justru berpotensi menjadi instrumen pengendalian narasi publik, memperburuk tren *shrinking civic space* yang telah menjadi perhatian masyarakat sipil nasional maupun internasional, serta membuka legitimasi tindakan represif terhadap warga sipil di ruang digital.⁸⁶

Kondisi tersebut sejak awal telah menjadi perhatian berbagai elemen masyarakat sipil sebagai implikasi revisi UU No. 34 Tahun 2004 tentang TNI. Salah satunya berupa penambahan peran TNI dalam OMSP berupa mendukung pemerintah dalam menghadapi ancaman siber. Dalam Daftar Inventaris Masalah (DIM) versi pemerintah, dijelaskan bahwa:⁸⁷

⁸⁵ Rubina Shaheen, "Gender and Surveillance: The Implications of Biometric Technologies for Privacy and Equity," *Journal of Gender, Power, and Social Transformation* 1, no. 3 (2024).

⁸⁶ SETARA Institute, "Patroli Siber TNI Mengarah pada Represi Digital," 9 September 2025, <https://setara-institute.org/patroli-siber-tni-mengarah-pada-represi-digital/>.

⁸⁷ Southeast Asia Freedom of Expression Network (SAFEnet), "Pernyataan Sikap SAFEnet: Tolak RUU TNI, Tolak Militerisasi Ruang Siber," 17 Maret 2025, <https://safenet.or.id/id/2025/03/tolak-ruu-tni-tolak-militerisasi-ruang-siber/>.

...Perang Siber tidak hanya menyerang infrastruktur secara fisik, namun juga dimensi virtual dan kognitif. Musuh/Lawan melakukan manipulasi sosial, polusi informasi, memperkuat narasi dengan ekspresi berlebihan untuk menyerang kerawanan kognitif. Konflik yang mengeksploitasi keunggulan informasi ini menjadi suatu senjata yang sangat berbahaya dengan cara memengaruhi keyakinan, sikap, dan perilaku masyarakat yang mengakibatkan konflik sosial, politik, dan ekonomi yang pada akhirnya mengancam keamanan negara.”

Persoalan tersebut memberikan gambaran yang kuat bahwa terjadi militerisasi ruang siber (*militarization of cyberspace*) sebagai implikasi revisi UU TNI tersebut. Militerisasi ruang siber merupakan upaya negara dalam mengonstruksi domain siber sebagai ancaman utama terhadap keamanan nasional, sehingga dapat digunakan untuk melegitimasi penerapan langkah-langkah berorientasi militer dalam menangani ancaman siber serta membenarkan pengembangan dan peningkatan berkelanjutan kapabilitas militer siber tanpa henti.⁸⁸

Dalam Rancangan Undang-Undang Keamanan dan Ketahanan Siber (RUU KKS), ELSAM juga telah menggarisbawahi bahwa sejumlah pengaturan dalam RUU *a quo* berpotensi membuka jalan bagi militerisasi ruang digital di Indonesia dengan memperluas peran dan kewenangan aparat keamanan dalam mengawasi aktivitas warga di internet. Kondisi tersebut, menjadi ekosistem yang ideal bagi militerisasi teknologi. Pendekatan dalam RUU tersebut terlalu berorientasi pada keamanan negara (*state-oriented*), bukan pada keamanan individu dan perlindungan warga.⁸⁹

Kondisi-kondisi demikian memperlihatkan paradoks demokrasi, khususnya terhadap hak-hak atas kebebasan berpendapat, berekspresi, dan juga berkumpul yang dijamin Konstitusi melalui Pasal 28 E ayat (3) UUD tahun 1945 yang menyatakan “Setiap orang berhak atas kebebasan berserikat, berkumpul, dan mengeluarkan pendapat.” Semestinya perlu dipahami bahwa lahirnya kebebasan berekspresi bertujuan untuk menghilangkan batasan dalam menyampaikan pendapat atau pandangan tertentu yang memiliki dampak negatif bagi kesejahteraan dan keadilan masyarakat. Kebebasan berekspresi digunakan untuk menyampaikan pandangan dan pendapat, baik antar individu atau kelompok.⁹⁰

3.2. Pelanggaran terhadap Ruang Privasi Warga Negara

3.2.1. Jaminan atas Ruang Privasi Warga Negara

Pengaturan regulasi yang menjamin ruang privasi warga negara menjadi semakin mendesak di tengah masifnya digitalisasi layanan publik, pengumpulan data oleh negara dan korporasi, serta penggunaan teknologi pengawasan. Lembaga Studi dan Advokasi

⁸⁸ SAFEnet, “Pernyataan Sikap SAFEnet: Tolak RUU TNI, Tolak Militerisasi Ruang Siber.”

⁸⁹ ELSAM, “Peneliti ELSAM Peringatkan Potensi Militerisasi Ruang Digital lewat RUU Keamanan dan Ketahanan Siber (RUU KKS),” 21 Oktober 2025, <https://www.elsam.or.id/teknologi-dan-ham/peneliti-elsam-peringatkan-potensi-militerisasi-ruang-digital-lewat-ruu-keamanan-dan-ketahanan-siber-ruu-kks->.

⁹⁰ Alifah Jasmine Kallista Remanu dkk., “Analisis Implikasi UU ITE terhadap Kebebasan Bereksprei di Ruang Digital: Studi Kasus Greenpeace Indonesia,” *Jurnal ISO: Jurnal Ilmu Sosial, Politik dan Humaniora* 4, no. 2 (2024).

Masyarakat (ELSAM) juga menegaskan bahwa dalam konteks data pribadi, yang terpenting justru adanya instrumen untuk memperkuat perlindungan data pribadi warga melalui arsitektur hukum yang mumpuni. Fokus perdebatannya juga bukan pada diskursus kedaulatan yang sifatnya tradisional (teritorial dan yurisdiksi), tetapi lebih pada kedaulatan individu pemilik data.⁹¹

Gambar 6 Ilustrasi Urgensi Payung Hukum Perlindungan Data Pribadi



Sumber: ELSAM

Privasi bukan sekadar isu teknis, melainkan prasyarat kebebasan berekspresi, kebebasan berpendapat, dan partisipasi demokratis. Karena itu, regulasi privasi yang jelas, akuntabel, dan berpihak pada hak warga negara merupakan fondasi penting untuk mencegah praktik otoritarianisme digital dan menjaga kualitas demokrasi. Pasal 28 G ayat (1) Undang-Undang Dasar 1945 menegaskan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda. Penjabarannya kemudian diwujudkan dalam beberapa peraturan yang berlaku, yang mencakup hal-hal berikut:⁹²

⁹¹ ELSAM, "UU Perlindungan Data Pribadi Mendesak untuk Menjamin Kedaulatan Individu di Ruang Siber," 2025, <https://www.elsam.or.id/siaran-pers/uu-perlindungan-data-pribadi-mendesak-untuk-menjamin-kedaulatan-individu-di-ruang-siber>.

⁹² Moh Bagas Fadhlil Dzil Ikrom dan Badrut Tamam, "Perlindungan Hukum Hak Privasi Warga Negara terhadap Kebocoran Data Pribadi di Indonesia," *Constitution Journal* 3, no. 2 (Desember 2024).

a. UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi

Berdasarkan Pasal 1 Ayat (2) UU Perlindungan Data Pribadi, perlindungan data pribadi adalah upaya menyeluruh untuk melindungi data pribadi dalam rantai pemrosesan data pribadi untuk menjamin hak konstitusional subjek data pribadi. Standar data pribadi yang dilindungi oleh UU PDP penting untuk memahami kriteria data pribadi yang harus dilindungi di bawah UU PDP agar memiliki perlindungan data yang tepat dan memenuhi kriteria data pribadi di bawah UU PDP. Pasal 1 Ayat 1 UU PDP menjelaskan data pribadi adalah data orang atau perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau terkombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik maupun nonelektronik.

b. UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

Perlindungan data pribadi dalam UU ini mencakup perlindungan data dari penggunaan yang tidak sah, perlindungan data oleh penyedia sistem elektronik, dan perlindungan data dari akses dan gangguan yang melanggar hukum. Dengan kata lain, segala penggunaan informasi yang melibatkan data pribadi seseorang melalui media atau Sistem Elektronik harus memperoleh izin dari individu yang bersangkutan.

c. Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi

Dalam regulasi ini, data pribadi merujuk pada informasi pribadi individu tertentu yang diolah, dipelihara, dan dijaga keakuratannya serta kerahasiaannya. Tidak hanya itu, dalam Pasal 5 ayat (4) menjelaskan, “tindakan pencegahan lainnya untuk menghindari terjadinya kegagalan dalam perlindungan Data Pribadi yang dikelolanya harus dilakukan oleh setiap Penyelenggara Sistem Elektronik, paling sedikit berupa kegiatan.

d. Peraturan Pemerintah Nomor 71 tahun 2019 Penyelenggaraan Sistem dan Transaksi Elektronik

Dalam PP ini, istilah ‘Penyelenggara Sistem Elektronik’ merujuk kepada individu, entitas negara, badan usaha, dan masyarakat yang menyediakan Sistem Elektronik. Mereka bertanggung jawab atas penyediaan, pengoperasian dan/atau pengelolaan sistem elektronik, baik secara sendiri-sendiri maupun bersama-sama, untuk kepentingan pengguna sistem elektronik, baik untuk kepentingan sendiri maupun untuk kepentingan pihak lain.

Berbagai perlindungan hukum terhadap hak privasi warga negara Indonesia, telah diatur dalam berbagai peraturan perundang-undangan di Indonesia. Perlindungan data pribadi telah diakui sebagai salah satu jenis HAM dan diakomodir dalam instrumen hukum internasional. Dalam hal ini, perlindungan data pribadi merupakan suatu irisan dari hak atas informasi dan hak atas privasi melalui proses evolusi yang panjang sejak diakuinya HAM melalui *The Universal Declaration of Human Rights* (UHDR) 1948. Pasal 12 UDHR secara spesifik mengatur mengenai perlindungan hak privasi seseorang, yaitu, “*No one shall be subjected to arbitrary interference with his privacy, family, or correspondence,*

*nor to attack upon his honours and reputation. Everyone has the right to the protection of the law against such interference or attacks.*⁹³

Istilah privasi dalam pasal tersebut merupakan *umbrella terms* yang dikaitkan dengan perlindungan keluarga, tempat tinggal, korespondensi atas kehormatan dan nama baiknya. Secara substantif, dapat dilihat bahwa UDHR memberikan perlindungan yang sangat luas mengenai hak privasi. *Pertama, physical privacy*, yang bertujuan untuk memberikan perlindungan privasi yang berhubungan dengan tempat tinggal seseorang.

Kedua, decisional privacy, yang bertujuan untuk memberikan perlindungan privasi terhadap seseorang untuk dapat menentukan kehidupannya sendiri termasuk kehidupan keluarganya. *Ketiga, dignity*, yang bertujuan untuk memberikan perlindungan privasi berkaitan dengan harga diri seseorang termasuk nama baik dan reputasi seseorang. *Keempat, informational privacy*, yang bertujuan untuk memberikan perlindungan privasi terhadap seseorang untuk dapat melakukan dan menyimpan data pribadi miliknya.⁹⁴

Jika perhatikan, rumusan Pasal 28G ayat (1) UUD 1945 memiliki nuansa perlindungan yang sama dengan rumusan *Article 12* UDHR yang kemudian diadopsi ke dalam *Article 17* ICCPR yang telah disahkan atau diratifikasi dalam UU No. 12 Tahun 2005 tentang pengesahan yang secara eksplisit memberikan jaminan terhadap hak atas privasi. Dalam Putusan MK No. 50/PUU-VI/2008, Mahkamah Konstitusi memberikan terjemahan atas *Article 12* UDHR dan *Article 17* ICCPR yaitu kata *privacy* diterjemahkan sebagai urusan pribadi/ masalah pribadi, bahwa:

*Tidak seorang pun boleh diganggu urusan pribadinya, keluarganya, rumah tangganya, atau hubungan surat-menyuratnya, dengan sewenang-wenang, juga tidak diperkenankan melakukan pelanggaran atas kehormatannya dan nama baiknya. Setiap orang berhak mendapat perlindungan hukum terhadap gangguan-gangguan atau pelanggaran seperti ini.*⁹⁵

Akan tetapi, meskipun sudah ada payung hukum yang jelas, praktik pelaksanaan undang-undang tersebut sering kali menemui kendala dalam menanggulangi masalah kebocoran data yang semakin marak. Informasi yang dibocorkan meliputi Nomor Induk Kependudukan (NIK), Kartu Keluarga (KK), nama lengkap, dan data pribadi lainnya. Kejadian ini mengungkapkan betapa rentannya data pribadi warga negara dalam sistem elektronik yang digunakan oleh pemerintah dan lembaga negara. Meski kebocoran

⁹³ Terj: Tidak seorang pun boleh dikenai campur tangan sewenang-wenang terhadap privasinya, keluarganya, atau korespondensinya, maupun serangan terhadap kehormatan dan reputasinya. Setiap orang berhak atas perlindungan hukum terhadap campur tangan atau serangan semacam itu. Asbjørn Eide, *The Universal Declaration of Human Rights: A Commentary* (Oslo: Scandinavian University Press, 1992), 188.

⁹⁴ Eide, *The Universal Declaration of Human Rights*, 188.; Elfian Fauzi dan Nabila Alif Radika Shandy, "Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi," *LEX Renaissance* 7, no. 3 (7 Juli 2022): 445–461.

⁹⁵ Aditiya Putra, "Apakah Hak atas Privasi Termasuk HAM?" *Hukumonline.com*, 3 Februari 2025, <https://www.hukumonline.com/klinik/a/apakah-hak-atas-privasi-termasuk-ham-lt4f5f850ec2388/>.

tersebut sudah dilaporkan dan mendapat perhatian publik, upaya pemerintah dalam menangani kasus ini masih dirasa belum cukup efektif.⁹⁶

3.2.2. Budaya Pengawasan: Perubahan Paradigma Perlindungan Warga menjadi Paradigma Kecurigaan terhadap Warga

Selain pelanggaran terhadap kebebasan berekspresi dan berpendapat, salah satu hak yang paling rentan tergerus akibat fenomena militerisasi teknologi ini adalah hak atas privasi. Modus operandi *cybercrime* yang semakin canggih dan menunjukkan tingkat kompleksitas yang tinggi sangat berpotensi dilakukan melalui penyalahgunaan teknologi di bidang pengelolaan data dan informasi, salah satunya adalah pembobolan dan pencurian data pribadi. Dalam konteks modern, pelanggaran terhadap hak privasi tidak lagi semata-mata terjadi melalui penyadapan fisik atau pengintaian konvensional, melainkan melalui penggunaan perangkat digital, data, dan sistem keamanan berbasis intelijen dengan orientasi militeristik untuk tujuan pengawasan (*surveillance*).

Angus Willoughby (2017) menggunakan term teknologi biometrik (*biometric technology*) sebagai teknologi yang menimbulkan kekhawatiran hak asasi manusia.⁹⁷ Sebab teknologi biometrik sering dikaitkan dengan pelanggaran privasi, terutama ketika diterapkan dalam konteks pengawasan, karena teknologi ini memungkinkan pengelola untuk mengidentifikasi seseorang, atau memverifikasi identitas seseorang, di kemudian hari.⁹⁸

⁹⁶ Moh Bagas Fadhlil Dzil Ikrom dan Badrut Tamam, "Perlindungan Hukum Hak Privasi Warga Negara terhadap Kebocoran Data Pribadi di Indonesia," *Constitution Journal* 3, no. 2 (Desember 2024).

⁹⁷ Angus Willoughby, "Biometric Surveillance and the Right to Privacy," 5 Oktober 2017, <https://technologyandsociety.org/biometric-surveillance-and-the-right-to-privacy/>.

⁹⁸ Dalam tulisannya, Willoughby menjelaskan bahwa Biometrika mengacu pada proses pencatatan, pengukuran, dan analisis berbagai fitur fisiologis manusia. Cakupan fitur yang dapat dicakup biometrika adalah "mencakup semua, dan mencakup penampilan, perilaku, dan kondisi kognitif". Ciri-ciri fisiologis tertentu bersifat permanen, unik, dan universal. Ciri-ciri ini dikenal sebagai "karakteristik biometrik". Karakteristik tersebut biasanya diukur oleh rangkaian sensor dan disimpan dalam basis data sebagai "templat". Sesuai dengan tujuan pengelola sistem biometrik, templat memungkinkan pengelola untuk mengidentifikasi seseorang, atau memverifikasi identitas seseorang, di kemudian hari. Willoughby, "Biometric Surveillance and the Right to Privacy."

Gambar 7 Ilustrasi Autentikasi, Identifikasi, dan Verifikasi Biometrik



Sumber: *recfaces.com*

Meskipun banyak diklaim berkontribusi terhadap keberhasilan penguatan pertahanan, misalnya di Amerika Serikat, militer dan badan intelijen semakin banyak menerapkan teknologi biometrik dalam kegiatan intelijen, pengawasan, dan pengintaian (ISR), serta telah melaporkan keberhasilan lain yang timbul dari penggunaan biometrik, seperti pengumpulan intelijen alat peledak rakitan dan operasi anti-pembajakan.⁹⁹ Dalam konteks ini, biometrik menjadi bagian dari strategi yang lebih luas yang menggabungkan identifikasi melalui teknologi biometrik dengan metode ISR lainnya untuk mengidentifikasi, melacak, atau membuat profil seseorang. Penggabungan berbagai metode tersebut dapat memperluas kemampuan pengawasan terhadap individu dan meningkatkan risiko pelanggaran privasi. Tergantung pada sifat dan implementasi teknologi biometrik tertentu, penggunaan teknologi tersebut dapat melanggar kewajiban hak asasi manusia internasional suatu negara. Lebih spesifiknya, masih belum pasti bagaimana teknologi tersebut berinteraksi dengan hak asasi manusia terkait privasi.¹⁰⁰

David Lyon (2018), seorang sosiolog dari Queen's University, menjelaskan bahwa sejak peristiwa 9/11 hingga kebocoran data Snowden, pengawasan mendominasi agenda pemerintah global hingga berita utama. Pengawasan bertransformasi, tidak hanya sebatas dilakukan terhadap eksistensi seseorang, tetapi sampai kepada sesuatu yang

⁹⁹ Willoughby, "Biometric Surveillance and the Right to Privacy."

¹⁰⁰ Willoughby, "Biometric Surveillance and the Right to Privacy."

individu tersebut lakukan dalam kehidupan sehari-hari. Kondisi ini, menurut David Lyon, merupakan bagian dari budaya pengawasan.

Potret masifnya budaya pengawasan, salah satunya dapat dilihat di China. Mulai dari jalanan yang dipenuhi kamera hingga aplikasi yang memerlukan identifikasi biometrik, hingga penggunaan pengenalan wajah telah berkembang di negara ini. Kondisi demikian memicu kekhawatiran masyarakat, bahkan survei yang dilakukan *Beijing News Think Tank*, menemukan dari 1.515 responden warga China, 87,46 persen responden menentang penggunaan teknologi pengenalan wajah di zona komersial.¹⁰¹

Gambar 8 Potret Kontroversi Teknologi Biometrik di China terhadap HAM



Sumber: *South China Morning Post*

Budaya ini telah menormalisasi pengawasan, sehingga kita tunduk pada pengawasan dan percaya bahwa tidak menyembunyikan apa pun. David Lyon menjelaskan bahwa ketika negara memiliki kemampuan untuk mengumpulkan dan menganalisis data dalam skala besar, warga negara kehilangan otonomi dan agensi terhadap data pribadi mereka. Kondisi ini mengubah relasi antara negara dan masyarakat menjadi relasi hierarkis berbasis kontrol, bukan kepercayaan.¹⁰²

¹⁰¹ South China Morning Post, "Facial Recognition Is Used in China for Everything from Refuse Collection to Toilet Paper Dispensers and Its Citizens Are Growing Increasingly Alarmed, Survey Shows," 2021, <https://www.scmp.com/tech/innovation/article/3119281/facial-recognition-used-china-everything-refuse-collection-toilet>.

¹⁰² David Lyon, *The Culture of Surveillance: Watching as a Way of Life* (Cambridge: Polity Press, 2018), <https://www.perlego.com/book/1536337/the-culture-of-surveillance-watching-as-a-way-of-life-pdf>.

Lebih jauh, militerisasi teknologi memperlebar jarak antara keamanan dan kebebasan, serta mengubah paradigma perlindungan warga menjadi paradigma kecurigaan terhadap warga. Dalam konteks demokrasi, hal ini bertentangan dengan prinsip negara hukum (*rule of law*) yang menempatkan individu sebagai subjek, bukan objek kekuasaan negara. Akibatnya, kepercayaan publik terhadap institusi keamanan dapat terkikis, dan legitimasi negara dalam menjalankan fungsi keamanan menjadi dipertanyakan.

Dalam konteks Indonesia, keamanan ruang privasi masyarakat bahkan semakin sulit dengan kondisi keroposnya sistem keamanan data berbagai lembaga negara, sehingga mengakibatkan kebocoran data pribadi. Misalnya kebocoran data BPJS Kesehatan pada Mei 2021 yang disusul dengan penjualan data peserta di Raid Forums seharga 0,15 Bitcoin. Kemudian kebocoran data 2,3 juta warga Indonesia dari Komisi Pemilihan Umum (KPU) pada Mei 2020. Data yang dibocorkan termasuk nama, alamat, nomor ID, tanggal lahir, dan lainnya.

Selain itu, temuan SAFEnet (2020) menunjukkan bahwa media digital juga digunakan sebagai sarana represi terhadap masyarakat sipil, antara lain melalui berbagai bentuk serangan digital. Berdasarkan pemantauan selama 2020, terdapat 147 insiden serangan digital. Puncak serangan digital terjadi pada Oktober 2020 dengan jumlah insiden sebanyak 41 kali. Banyaknya peristiwa di bulan Oktober berkaitan dengan situasi politik Indonesia. Pada Oktober 2020, Pemerintah Indonesia mengesahkan Undang-undang Cipta Kerja yang disebut juga Undang-Undang sapu jagat (*Omnibus Law*). Pengesahan UU Cipta Kerja memicu penolakan di kalangan masyarakat sipil yang bahkan menjadi *trending topic* di Twitter. Masifnya suara penolakan itu dibarengi dengan maraknya serangan digital terhadap mahasiswa, aktivis, dan organisasi masyarakat sipil.¹⁰³

Secara umum, serangan digital ini ada dua kategori. Pertama, serangan secara kasar (*hard attack*) dengan karakter melibatkan peralatan dan teknik tertentu untuk menyerang target atau bahkan mengambil alih aset korban. Contoh serangan yang masuk kategori ini adalah peretasan, penyadapan, dan serangan DDoS (*distributed denial of service*). Tidak setiap orang bisa melakukan serangan secara kasar ini karena memerlukan teknologi dan kemampuan tertentu.¹⁰⁴

Kedua, serangan secara halus (*soft attack*). Serangan melalui metode ini lebih bertujuan untuk mengintimidasi psikologis korban (*psywar*) atau menjatuhkan kredibilitas korban di mata publik. Karena itu, serangan secara halus ini harus dilakukan secara terbuka melalui media sosial oleh (para) pelaku, baik profil anonim maupun nyata. Contoh serangan dalam kategori ini adalah penyebaran identitas pribadi tanpa persetujuan (*doxing*), peniruan akun (*impersonasi*), dan penyerbuan (*trolling*) melalui komentar atau unggahan.¹⁰⁵

Sementara, berbagai kasus dalam militerisasi teknologi yang mengancam ruang privasi warga negara yang terjadi di Myanmar dapat menjadi pembelajaran. Pemerintah junta

¹⁰³Southeast Asia Freedom of Expression Network (SAFEnet), *Laporan Situasi Hak-hak Digital Indonesia 2020: Represi Digital di Tengah Pandemi* (Denpasar: Southeast Asia Freedom of Expression Network (SAFEnet), 2021).

¹⁰⁴ SAFEnet, *Laporan Situasi Hak-hak Digital Indonesia 2020*.

¹⁰⁵ SAFEnet, *Laporan Situasi Hak-hak Digital Indonesia 2020*.

Myanmar memasang kamera buatan China yang memiliki kemampuan pengenalan wajah di lebih banyak kota di seluruh negeri, dengan alasan untuk menjaga keamanan perdamaian sipil. Namun, para pegiat HAM yang mengetahui proyek-proyek tersebut, justru menaruh kekhawatiran besar. Sebab alat tersebut dapat digunakan untuk menindak para aktivis dan kelompok-kelompok perlawanan, yang keduanya telah ditetapkan sebagai teroris oleh junta setelah kudeta. Militer dan polisi dapat menggunakannya untuk melacak pergerakan mereka, mencari tahu hubungan antara aktivis, mengidentifikasi rumah aman dan tempat berkumpul lainnya.¹⁰⁶

Gambar 9 Pemerintah Junta Myanmar Memasang Kamera Buatan China



Sumber: *Reuters*

Human Rights Watch menegaskan bahwa akses junta militer ke sistem kamera publik baru yang dilengkapi dengan teknologi pengenalan wajah dan pengenalan plat nomor menimbulkan ancaman serius terhadap hak-hak dasar warga. Meskipun disebut untuk membangun inisiatif Kota Aman, sejak Desember 2020 pemerintah bahkan telah menggunakan sistem 335 kamera pengintai di delapan kotapraja di ibu kota, Naypyidaw. Teknologi tersebut justru memungkinkan pemerintah untuk memantau kebiasaan dan

¹⁰⁶ VOA Indonesia, "Perketat Pengawasan, Junta Myanmar Pasang CCTV Canggih China di Lebih Banyak Kota," 7 Juli 2022, <https://www.voaindonesia.com/a/perketat-pengawasan-junta-myanmar-pasang-cctv-canggih-china-di-lebih-banyak-kota-/6653414.html>.

pergerakan masyarakat, sehingga berpotensi menimbulkan efek samping yang merugikan hingga mengancam ruang privasi masyarakat.¹⁰⁷

Persoalan lainnya berkaitan dengan tidak jelasnya siapa pejabat maupun pihak yang akan diberi akses ke data tersebut. Di Myanmar, teknologi pengenalan wajah dan pelat nomor kendaraan diluncurkan tanpa konsultasi publik maupun transparansi yang memadai. Akibatnya, tidak terdapat kejelasan mengenai langkah-langkah yang direncanakan pihak berwenang untuk memitigasi potensi dampak penggunaan teknologi tersebut terhadap HAM, khususnya hak atas privasi.¹⁰⁸

Selain itu, perlu dipahami juga bahwa teknologi ini juga dapat digunakan untuk mengisolasi individu secara diskriminatif atau sewenang-wenang, termasuk berdasarkan etnis atau agama mereka. Kondisi di Tiongkok juga dapat menjadi pembelajaran berikutnya, karena pengenalan wajah dan pengenalan plat nomor telah digunakan untuk tujuan pengawasan massal. Di wilayah Xinjiang, pemerintah Tiongkok menggunakan berbagai teknologi, termasuk pengenalan wajah, kamera pengawas, dan program data besar untuk memantau dan melacak etnis Uighur dan warga negara lainnya. Siapa pun yang ditandai sebagai “bermasalah” berdasarkan kriteria yang tidak jelas dapat dikirim ke kamp pendidikan politik dan menjadi sasaran indoktrinasi politik.¹⁰⁹

4. Bagaimana Pengaturan dan Pertanggungjawaban Mengenai Militerisasi Teknologi?

Integrasi teknologi digital—seperti sistem pengawasan (*surveillance systems*), senjata siber (*cyber weapons*), kecerdasan buatan, sistem persenjataan otonom, dan *big data analytics*—ke dalam struktur militer tidak hanya mempercepat transformasi operasional, tetapi juga memperluas potensi dampak terhadap hak asasi manusia. Laju adopsi teknologi ini juga sering kali lebih cepat daripada perkembangan regulasi, sehingga menciptakan kesenjangan tata kelola yang menimbulkan permasalahan serius dalam aspek pengaturan, akuntabilitas, dan transparansi.

Dalam konteks Indonesia, akuntabilitas dan transparansi dalam bidang pertahanan negara sudah menjadi isu lama tanpa kejelasan perkembangannya hingga kini. Arifianto (2005) dalam penelitiannya berjudul *Sistem Pengelolaan Anggaran Belanja Militer di Indonesia: Tinjauan Aspek Pengendalian, Transparansi dan Akuntabilitas Publik*, menunjukkan bahwa sistem pengelolaan anggaran belanja dan keuangan Dephan-TNI memiliki kelemahan inheren yang berpengaruh pada efektivitas sistem yaitu sistem otorisasi anggaran dan pendanaan yang terlalu kaku, birokratis, dan tidak fleksibel; tidak adanya pembatasan tugas yang mampu mengatur pengendalian internal; dan sistem

¹⁰⁷ Human Rights Watch, “Myanmar: Facial Recognition System Threatens Rights: Camera Surveillance, Mass Data Collection Bolsters Abusive Junta,” 12 Maret 2021, <https://www.hrw.org/news/2021/03/12/myanmar-facial-recognition-system-threatens-rights>.

¹⁰⁸ Human Rights Watch, “Myanmar: Facial Recognition System Threatens Rights.”

¹⁰⁹ Human Rights Watch, “Myanmar: Facial Recognition System Threatens Rights.”

pertanggungjawaban keuangan yang kurang transparan dan akuntabel yang berisiko menimbulkan penyimpangan.¹¹⁰

Dalam konteks regulasi, baik publik maupun negara, terdapat dilema antara kebutuhan untuk menjaga kerahasiaan dengan tata kelola demokratis yang menempatkan akuntabilitas dan transparansi sebagai prinsip utama. Bahkan dalam kerangka hukum nasional melalui UU No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik, pada Pasal 17 huruf c, dijelaskan terdapat informasi yang dikecualikan dari publik, seperti informasi yang berkaitan dengan pertahanan dan keamanan negara, yakni:

1. Informasi tentang strategi, intelijen, operasi, taktik dan teknik yang berkaitan dengan penyelenggaraan sistem pertahanan dan keamanan negara, meliputi tahap perencanaan, pelaksanaan dan pengakhiran atau evaluasi dalam kaitan dengan ancaman dari dalam dan luar negeri.
2. Dokumen yang memuat tentang strategi, intelijen, operasi, teknik dan taktik yang berkaitan dengan penyelenggaraan sistem pertahanan dan keamanan negara yang meliputi tahap perencanaan, pelaksanaan dan pengakhiran atau evaluasi.
3. Jumlah, komposisi, disposisi, atau dislokasi kekuatan dan kemampuan dalam penyelenggaraan sistem pertahanan dan keamanan negara serta rencana pengembangannya.
4. Gambar dan data tentang situasi dan keadaan pangkalan dan/atau instalasi militer; dan
5. Data-data perkiraan kemampuan militer dan pertahanan negara lain terbatas pada segala tindakan dan/atau indikasi negara tersebut yang dapat membahayakan kedaulatan NKRI dan/atau data terkait kerjasama militer dengan negara lain yang disepakati dalam perjanjian tersebut sebagai rahasia atau sangat rahasia.

Ketentuan Pasal 17 huruf c Undang-Undang No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik (KIP) yang memberikan pengecualian atas informasi terkait pertahanan dan keamanan negara pada prinsipnya dimaksudkan untuk melindungi kerahasiaan strategis yang dapat mengancam keselamatan nasional apabila dibuka kepada publik. Namun, dalam praktik tata kelola sektor pertahanan di Indonesia, ketentuan pengecualian tersebut sering dijadikan justifikasi normatif untuk membatasi akses publik secara berlebihan terhadap informasi yang sebenarnya tidak termasuk kategori sensitif, seperti alokasi anggaran, proses pengadaan, dan evaluasi kinerja program pertahanan.¹¹¹

Dampaknya sangat serius terhadap tata kelola demokratis. Sebab sektor pertahanan merupakan domain yang secara tradisional dianggap memiliki tingkat sensitivitas dan kerahasiaan tinggi. Bahkan tidak sedikit rapat-rapat antara Komisi I DPR bersama TNI digelar tertutup dengan dalih tersebut, termasuk saat rapat-rapat yang membahas soal

¹¹⁰ Yuniar Arifianto, *Sistem Pengelolaan Anggaran Belanja Militer di Indonesia: Tinjauan Aspek Pengendalian, Transparansi dan Akuntabilitas Publik* (Depok: Fakultas Ekonomi dan Bisnis Universitas Indonesia, 2005), <https://lib.ui.ac.id/detail?id=83595&lokasi=lokal>.

¹¹¹ Kondisi tersebut, di antaranya, kental terlihat pada momen debat III Calon Presiden pada Pemilu 2024 lalu yang mengangkat tema pertahanan dan keamanan. Prabowo Subianto, selaku salah satu calon Presiden, berulang kali memberikan dalih rahasia negara terhadap topik-topik yang berkaitan anggaran alutsista, serta isu-isu pertahanan lainnya.

pengadaan alutsista.¹¹² Paradoksnya, ketika pemerintah menekankan perihal rahasia negara, proses pengadaan alutsista ujung-ujungnya juga akan dipublikasi melalui berbagai media massa maupun lembaga yang menjual senjata tersebut ke Indonesia, termasuk soal harga, spesifikasi, dan tahun produksi.¹¹³

Tingkat kerahasiaan yang tinggi dalam sektor pertahanan, terutama dalam konteks negara-negara berkembang seperti Indonesia, secara struktural berkontribusi terhadap semakin tidak terkendalinya proses militerisasi teknologi. Kerahasiaan yang dipraktikkan oleh sektor militer—melalui pembatasan informasi, minimnya mekanisme pelaporan, serta absennya transparansi dalam proses pengadaan, uji coba, dan penggunaan teknologi—menciptakan ruang kebijakan yang sulit diawasi oleh otoritas sipil maupun publik. Ketika negara menggunakan sistem pengawasan digital atau alat siber secara luas dengan dalih keamanan tanpa mekanisme transparansi yang kuat, maka dapat terjadi erosi terhadap kebebasan sipil dan privasi.

Mengingat kompleksitas persoalan dan potensi dampaknya terhadap kemunduran demokrasi, pengaturan mengenai militerisasi teknologi menjadi kebutuhan mendesak. Pengaturan tersebut diperlukan untuk memastikan bahwa penggunaan teknologi pertahanan dilakukan berdasarkan prinsip legalitas, kebutuhan, dan proporsionalitas, serta berada di bawah mekanisme pengawasan dan pertanggungjawaban yang efektif. Dengan kerangka regulasi yang memadai, negara dapat menjaga keseimbangan antara kepentingan keamanan nasional dan perlindungan hak-hak warga negara, sekaligus mencegah normalisasi praktik pengawasan yang tidak akuntabel dan berpotensi merusak demokrasi.

4.1. Bagaimana Penggunaan Anggaran dapat Dipertanggungjawabkan?

Pengaturan pertama berkaitan dengan transparansi anggaran. Dalam kerangka demokrasi, transparansi penganggaran pertahanan tidak hanya berfungsi sebagai instrumen manajerial, tetapi juga sebagai mekanisme akuntabilitas politik. Keterbukaan anggaran memungkinkan parlemen dan publik untuk menilai apakah prioritas belanja pertahanan selaras dengan kepentingan keamanan nasional dan nilai-nilai konstitusional, termasuk perlindungan hak asasi manusia.

Namun, upaya menuju kondisi ideal tersebut cukup terjal. Data yang tersedia terkait anggaran pertahanan dan proses penganggaran sangat terbatas dan sering kali tidak dapat diandalkan. Tekanan publik dan media terhadap pemerintah untuk mengungkapkan informasi pun pada umumnya terbatas. Para pemimpin sering kali menahan informasi terkait pertahanan dengan alasan bahwa terlalu banyak informasi yang tersedia merupakan ancaman bagi keamanan negara. Retorika ini sekarang banyak

¹¹² Detik.com, "Rapat Komisi I DPR, Panglima TNI Tertutup Saat Bahas Alutsista," 22 Oktober 2024, <https://news.detik.com/berita/d-5560339/rapat-komisi-i-dpr-panglima-tni-tertutup-saat-bahas-alutsista>; Fachri Audhia Hafiez, "Rapat Bahas Anggaran Alutsista Menhan dengan Komisi I DPR Digelar Tertutup," *MetroTVNews.com*, 12 Juni 2024, <https://www.metrotvnews.com/read/bD2C1Qj6-rapat-bahas-anggaran-alutsista-menhan-dengan-komisi-i-dpr-digelar-tertutup>.

¹¹³ Vitorio Mantalean dan Ardito Ramadhan, "Imparsial: Pengadaan Alutsista Rawan Korupsi dengan Dalih Rahasia Pertahanan," *Kompas.com*, 10 Desember 2024.

digunakan di beberapa negara di dunia, seperti Tiongkok, di mana pihak berwenang bahkan tidak mempublikasikan anggaran negara yang telah disetujui.¹¹⁴

Faktor berikutnya dapat berupa kurangnya kapasitas dan pemahaman SDM, sehingga menghambat kemampuan banyak pemerintah untuk mempublikasikan informasi anggaran pertahanan. Kondisi tersebut semakin rumit ketika terbatasnya definisi pengeluaran militer yang diterima secara universal, yang mempersulit proses penentuan komposisi yang tepat dari item anggaran pertahanan yang akan diumumkan kepada publik.¹¹⁵

Akuntabilitas dan transparansi anggaran yang digunakan dalam penyediaan teknologi militer perlu dipandang sebagai bagian dari hak Konstitusional warga negara, sebagaimana diatur dalam Pasal 28F UUD NRI 1945, yakni:

“Setiap orang berhak untuk berkomunikasi dan memperoleh informasi untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia.”

Pasal ini menegaskan bahwa keterbukaan informasi bukan sekadar kebijakan administratif, melainkan hak konstitusional yang melekat pada warga negara dan menjadi prasyarat penting bagi akuntabilitas, transparansi, dan kontrol sipil dalam negara demokratis.

Selain itu, perlu dipahami bahwa pertahanan dan keamanan merupakan layanan publik yang diselenggarakan negara dan dibiayai oleh pajak warga negara. Karena itu, hubungan antara negara dan warga dalam sektor ini bersifat kontraktual dalam kerangka demokrasi: dana publik yang dihimpun melalui pajak menuntut pertanggungjawaban publik. Oleh karena itu, hak warga negara untuk mengetahui bagaimana uang pajaknya digunakan tidak dapat dikesampingkan dengan dalih keamanan nasional. Meskipun juga dipahami bahwa terdapat informasi operasional dan taktis tertentu perlu dilindungi demi keselamatan negara.

Namun, akuntabilitas tidak harus mengesampingkan kerahasiaan informasi yang memang perlu dilindungi. Transparansi anggaran pertahanan tidak selalu berarti membuka seluruh informasi kepada publik, tetapi juga mencakup mekanisme lain yang memungkinkan pengawasan dan pertanggungjawaban tetap berjalan. Setidaknya, terdapat dua hal yang dapat dilakukan untuk mewujudkannya. Pertama, informasi mengenai pengeluaran pertahanan dan investasi dalam layanan publik alternatif, yakni berfokus pada bagaimana tingkat pengeluaran pertahanan memengaruhi prioritas pembangunan lainnya di mana intervensi negara diperlukan. Misalnya, Dwight D. Eisenhower mencatat pada tahun 1953 bahwa biaya satu pesawat pembom sama dengan biaya membangun 30 sekolah, dua pembangkit listrik, atau 2 rumah sakit.¹¹⁶

¹¹⁴ Mariya Gorbanova dan Leah Wawro, *The Transparency of National Defence Budgets: An Initial Review* (London: Transparency International UK, 2011).

¹¹⁵ Gorbanova dan Wawro, *The Transparency of National Defence Budgets*.

¹¹⁶ Gorbanova dan Wawro, *The Transparency of National Defence Budgets*.

Kedua, untuk meningkatkan transparansi anggaran pertahanan sekaligus mengurangi risiko terungkapnya informasi terkait keamanan yang sangat sensitif, Korea Selatan menyusun 3 kategori informasi anggaran pertahanan, yang mengacu pada tingkat kerahasiaannya. Pada Kategori A, pos anggaran disajikan untuk dibahas kepada seluruh Majelis Nasional (*National Assembly*) dalam bentuk agregat. Lalu pada Kategori B, pos anggaran diungkapkan kepada anggota Komite Pertahanan Nasional Majelis Nasional (*National Assembly Committee of National Defence*) yang ditunjuk dalam bentuk yang lebih rinci dan terpisah. Kemudian pada Kategori C, pos-pos tersebut diuraikan lebih lanjut dan hanya disajikan kepada Komite Pertahanan Nasional (*Committee of National Defence*). Sebelumnya, anggota legislatif hanya diberikan angka total untuk diperdebatkan.¹¹⁷

Lebih lanjut, perjalanan Korea Selatan dalam penguatan transparansi dan akuntabilitas anggaran pertahanan dapat menjadi salah satu referensi. Sebab selain mengategorikan informasi anggaran pertahanan, Korea Selatan juga memiliki 4 (empat) strategi untuk meningkatkan transparansi pertahanan di dalam negeri, yakni:¹¹⁸

1. Kementerian Pertahanan Nasional (*Ministry of National Defense/MND*) memberikan informasi kepada publik melalui halaman utama situs webnya. Halaman utama MND memperkenalkan kebijakan pertahanan kepada publik melalui unggahan bagan organisasi MND, berita pertahanan, dan makalah kebijakan utama. Secara khusus, MND terus berupaya menginformasikan kepada publik tentang dukungannya terhadap warga sipil dan mencari masukan publik melalui "*Participation Plaza*" bagian tanya jawab untuk menjawab kekhawatiran publik tentang pertahanan. Selain itu, MND menyediakan berita pertahanan kepada 3.000 pakar sipil dan pensiunan perwira melalui Manajemen Hubungan Pelanggan Publik (*Public Customer Relationship Management/ PCRM*).
2. MND mengadakan konferensi pers rutin 2 (dua) kali sehari untuk menjelaskan isu-isu pertahanan terkini. Pemantauan media yang terus menerus menjadi cara terbaik untuk meningkatkan transparansi pertahanan. Mengingat Korea Selatan menghadapi Korea Utara secara militer, sebagian besar informasi pertahanannya diklasifikasikan sebagai rahasia negara. Akan tetapi, peningkatan kualitas transparansi pertahanan dapat dilakukan dengan memungkinkan pemantauan media. Juru bicara menjawab pertanyaan yang diajukan sebelumnya, menjelaskan isu-isu kepada publik, dan mengadakan sesi tanya jawab. Melalui pengarahannya ini, MND berupaya memastikan bahwa publik mendapatkan berita terkait pertahanan secara tepat waktu. Selain pengarahannya ini, MND menerbitkan *Korea Defense Daily*, yang menyediakan berita pertahanan kepada anggota militer aktif dan purnawirawan serta para ahli sipil.

¹¹⁷ Gorbanova, Mariya, dan Leah Wawro. *The Transparency of National Defence Budgets: An Initial Review*. London: Transparency International UK, 2011.

¹¹⁸ Beomchul Shin, *The Republic of Korea's Perspective on Defense Transparency*, Policy Brief No. 2011-1 (Northeast Asia Defense Transparency Project, University of California Institute on Global Conflict and Cooperation, Oktober 2011).

3. Ketiga, buku putih pertahanan, yang diterbitkan setiap dua tahun sekali, adalah publikasi terpenting yang memberikan penjelasan komprehensif tentang kebijakan pertahanan kepada publik. Pada tahun sebelum penerbitan, MND meminta masukan ahli dari lembaga think tank Korea untuk meningkatkan kualitas buku putih berikutnya. Melalui upaya-upaya ini, MND memastikan bahwa materi dalam buku putih pertahanan diterima dengan baik oleh publik.
4. Keempat, Majelis Nasional (*National Assembly*) memainkan peran yang sangat penting dalam mempromosikan transparansi pertahanan melalui inspeksi tahunan dan pembahasan anggarannya. Inspeksi, yang berlangsung segera setelah tanggal 10 September setiap tahun, berlangsung selama 20 hari. Selama periode inspeksi, Majelis Nasional dapat meninjau berbagai isu kebijakan pertahanan, dan Kementerian Pertahanan harus menyediakan materi yang diminta oleh Majelis Nasional. Majelis Nasional juga dapat meluncurkan investigasi independen jika ditemukan pelanggaran serius dalam manajemen pertahanan.

Strategi Korea Selatan dalam memastikan akuntabilitas dan transparansi tetap terselenggara pada isu pertahanan dapat menjadi referensi bagi Indonesia. Sebab pembahasan anggaran pertahanan di Indonesia masih ditempatkan dalam rezim kerahasiaan yang berlebihan, baik oleh Presiden sebagai pemegang kekuasaan pemerintahan sekaligus panglima tertinggi, maupun oleh DPR sebagai lembaga representatif yang seharusnya menjalankan fungsi pengawasan anggaran. Dalih yang paling sering digunakan untuk membenarkan keterbatasan akses publik adalah “rahasia negara.”

Misalnya ketika Komisi I DPR RI menggelar rapat kerja dengan Kementerian Pertahanan (Kemhan), Panglima TNI, KSAD, KSAU, hingga KSAL pada 12 Juni 2024 yang membahas soal evaluasi anggaran 2024 hingga pembahasan RAPBN tahun anggaran 2025. Karena rapat membahas anggaran Kemhan serta TNI yang kaitannya dengan alutsista, akhirnya diputuskan secara tertutup.¹¹⁹ Hal serupa juga dilakukan tahun 2025, tepatnya pada 9 Juli 2025, ketika Menteri Pertahanan (Menhan) Sjafrie Sjamsoeddin bersama Panglima TNI Jenderal Agus Subiyanto telah melakukan rapat tertutup bersama Komisi I DPR RI. Rapat dilakukan untuk membahas rencana kerja dan anggaran tahun 2026.¹²⁰

Ketertutupan pembahasan anggaran pertahanan di Indonesia pada akhirnya juga mencapai titik yang problematik. Rapat-rapat antara pemerintah dan DPR digelar secara tertutup dengan dalih *rahasia negara*, namun pada saat yang sama publik justru “dikagetkan” oleh informasi bahwa anggaran pertahanan dinaikkan secara signifikan. Pola ini memperlihatkan paradoks serius dalam tata kelola demokrasi: keputusan fiskal

¹¹⁹ Dwi Rahmawati, “Bahas Anggaran Kemhan 2025, Rapat Komisi I DPR Digelar Tertutup,” *detikNews*, 12 Juni 2024, <https://news.detik.com/berita/d-7386957/bahas-anggaran-kemhan-2025-rapat-komisi-i-dpr-digelar-tertutup>.

¹²⁰ Adrial Akbar, “Rapat Tertutup di DPR, Menhan-Panglima TNI Usul Tambah Anggaran Rp 184 T,” *detikNews*, 9 Juli 2025, <https://news.detik.com/berita/d-8003834/rapat-tertutup-di-dpr-menhan-panglima-tni-usul-tambah-anggaran-rp-184-t>.

strategis diambil tanpa proses deliberasi publik yang memadai, tetapi dampak keuangannya dibebankan kepada masyarakat luas.

Salah satu contohnya terlihat dari hasil rapat tertutup pada Juli 2025, ketika Kementerian Pertahanan mengajukan penambahan anggaran sebesar Rp184 triliun.¹²¹ Dalam situasi seperti ini, klaim *rahasia negara* tidak lagi berfungsi sebagai perlindungan keamanan, melainkan sebagai tameng untuk menutup proses pengambilan keputusan dari pengawasan demokratis.¹²²

Pada akhirnya, publik dapat melihat dan memahami bahwa, dalam praktiknya, di Indonesia konsep *rahasia negara* dalam anggaran pertahanan tidak diperlakukan sebagai pengecualian yang bersifat terbatas (*narrowly tailored exception*), melainkan sebagai justifikasi umum untuk menutup hampir seluruh siklus penganggaran—mulai dari perencanaan, pembahasan, hingga evaluasi. DPR yang secara konstitusional memiliki kewenangan *budgetary oversight* cenderung mereproduksi logika eksekutif alih-alih mengoreksinya. Pembahasan anggaran pertahanan sering dilakukan dalam forum tertutup. Sementara di Korea Selatan, Majelis Nasional (*National Assembly*) justru memainkan peran yang sangat penting dalam mempromosikan transparansi pertahanan melalui inspeksi tahunan dan pembahasan anggarannya.

Selain itu, bentuk transparansi dan akuntabilitas Korea Selatan dalam bidang pertahanan juga diwujudkan melalui penerbitan *Defense White Paper* setiap dua tahun sekali sebagai bentuk pertanggungjawaban publik atas arah kebijakan pertahanan negara. Praktik ini menunjukkan bahwa negara dengan tingkat ancaman militer tinggi sekalipun tetap memandang transparansi sebagai bagian integral dari keamanan nasional, bukan sebagai ancaman terhadapnya.

Sebaliknya, Indonesia belum memiliki tradisi penerbitan buku putih pertahanan yang reguler dan mudah diakses publik. Akibatnya, publik kesulitan memahami keterkaitan antara ancaman yang dihadapi, strategi pertahanan yang dipilih, dan kenaikan anggaran yang diminta negara. Buku Putih Pertahanan Indonesia terakhir kali diterbitkan pada tahun 2015 oleh Kementerian Pertahanan Republik Indonesia. Tetapi sejak itu tidak ada edisi pembaruan yang dirilis secara resmi kepada publik.

Transparansi dan akuntabilitas anggaran pertahanan Korea Selatan perlu dicatat lahir dari sejarah panjang dan *political will* yang kuat. Ketika Kim Young Sam, presiden sipil pertama dalam lebih dari tiga dekade, menjabat pada tahun 1993, pemerintahannya menyingkirkan faksi-faksi di dalam militer, menyelidiki korupsi dalam pengadaan pertahanan, dan mempromosikan transparansi dalam pengeluaran pertahanan. Majelis Nasional dan pers independen bertindak dan melaporkan insiden dan korupsi yang terkait

¹²¹ Akbar, "Rapat Tertutup di DPR."

¹²² Ironisnya, sebagian alasan yang belakangan muncul untuk membenarkan kenaikan anggaran pertahanan adalah peningkatan kesejahteraan personel. Dalih ini justru menimbulkan pertanyaan mendasar: sejak kapan isu kesejahteraan prajurit—yang berkaitan dengan gaji, tunjangan, dan layanan dasar—dikategorikan sebagai *rahasia negara*? Tidak ada aspek operasional atau intelijen yang terancam ketika publik mengetahui arah kebijakan kesejahteraan aparaturnya.

dengan militer—tanpa terkecuali. Melalui proses-proses ini, transparansi pertahanan telah sangat ditingkatkan dari perspektif domestik.¹²³

Pada era pemerintahan Lee Myung Bak (2008-2013), transparansi pertahanan Korea Selatan terus ditingkatkan. Pemerintahan saat itu juga berupaya meningkatkan transparansi pertahanan dengan menyatakan “pertahanan untuk rakyat” sebagai dasar kebijakannya. Di bawah slogan ini, pemerintah berusaha memberikan lebih banyak informasi kepada publik dan mencari dukungan publik. Dalam menyediakan informasi terkait pertahanan untuk memenuhi permintaan publik, pemerintah Korea juga meningkatkan kerja sama dengan komunitas internasional.¹²⁴

Dalam konteks domestik, penganggaran pertahanan yang akurat dan transparan merupakan prasyarat penting untuk memastikan bahwa sumber daya negara dialokasikan secara efektif di antara berbagai fungsi yang dijalankan dalam sektor pertahanan dan keamanan. Tanpa perencanaan anggaran yang jelas dan terbuka, distribusi sumber daya berisiko timpang, tidak berbasis kebutuhan strategis, dan cenderung didorong oleh kepentingan birokrasi jangka pendek. Selain alasan domestik ini, proses penganggaran pertahanan yang transparan dapat memberikan manfaat regional dan internasional. Kerahasiaan yang berlebihan dapat menyebabkan tingkat ketidakpastian dan kecurigaan yang lebih tinggi di tingkat regional dan global.¹²⁵

4.2. Apakah Ada Pelanggaran Hukum dalam Pengadaan Alat-Alat Militer?

Pengadaan alat-alat militer merupakan salah satu area kebijakan publik yang paling rentan terhadap pelanggaran hukum karena melibatkan anggaran besar, tingkat kerahasiaan tinggi, serta relasi kuasa yang kuat antara aktor negara dan penyedia teknologi. Dalam konteks ini, pelanggaran hukum—seperti penyimpangan prosedur pengadaan, konflik kepentingan, *mark-up* anggaran, atau pengadaan tanpa dasar kebutuhan strategis yang jelas—tidak hanya berdampak pada kerugian keuangan negara, tetapi juga berpotensi melemahkan tata kelola pertahanan dan akuntabilitas demokratis. Ketika proses pengadaan berlangsung tanpa kepatuhan hukum yang ketat, ruang pengawasan publik dan parlementer menjadi semakin sempit, sehingga meningkatkan risiko penyalahgunaan kekuasaan.

Salah satu sorotan terhadap pengadaan alat-alat yang berkaitan dengan militerisasi teknologi tersebut dapat dilihat melalui laporan Amnesty International – bekerja sama dengan mitra medianya, Haaretz, Inside Story, Tempo, kolektif riset WAV, dan Woz – berjudul *A Web of Surveillance – Unravelling a murky network of spyware exports to Indonesia*. Laporan tersebut menunjukkan bahwa dalam kurun waktu 2017 hingga 2023, terdapat pola sistematis dalam pengadaan dan penggunaan teknologi pengawasan yang

¹²³ Shin, *The Republic of Korea's Perspective on Defense Transparency*.

¹²⁴ Shin, *The Republic of Korea's Perspective on Defense Transparency*.

¹²⁵ Gorbanova dan Wawro, *The Transparency of National Defence Budgets*.

sangat intrusif oleh sejumlah entitas di Indonesia,¹²⁶ baik yang berasal dari sektor negara maupun yang berelasi dengan kepentingan keamanan nasional.¹²⁷

Berbagai perangkat lunak mata-mata dan teknologi pengawasan canggih dilaporkan telah diimpor dan didistribusikan, mencerminkan meningkatnya ketergantungan pada instrumen digital untuk tujuan intelijen dan pengendalian keamanan. Di antara teknologi yang disebutkan adalah Pegasus—perangkat lunak mata-mata terkenal yang dikembangkan oleh NSO Group berbasis di Israel—serta Predator, *platform spyware* berkapasitas tinggi yang dikembangkan oleh konsorsium internasional Intellexa. Selain itu, laporan tersebut juga mengungkap keberadaan sistem infiltrasi siber Cyrus, produk vendor teknologi pengawasan Israel Saito Tech (juga dikenal sebagai Candiru), yang dirancang untuk menembus dan memantau perangkat digital secara tersembunyi.¹²⁸

Penjualan dan transfer perangkat lunak mata-mata dan teknologi pengawasan ini dimungkinkan melalui ekosistem yang tidak jelas dari para vendor, broker, dan pengecer pengawasan dengan struktur kepemilikan yang kompleks.¹²⁹ Sementara, Indonesia memiliki UU No. 16 Tahun 2012 tentang Industri Pertahanan yang semestinya menjadi kerangka dan landasan kebijakan bagi berbagai pengadaan alat-alat pertahanan-keamanan di Indonesia.¹³⁰ Melalui ketentuan Pasal 2, dapat dipahami bahwa prioritas menjadi asas utama dalam Penyelenggaraan Industri Pertahanan, begitu pun akuntabilitas juga menjadi salah satu asas. Ketentuan ini dapat menjadi gambaran bahwa Penyelenggaraan Industri Pertahanan tidak sekedar berlandaskan pada asas kerahasiaan, sehingga sulit disentuh pertanggung-jawabannya.

UU *a quo* melalui Pasal 43 juga mengatur perihal pengadaan alat peralatan pertahanan dan keamanan dari luar negeri atau produk luar negeri. Namun pengadaan tersebut tidak dapat dilakukan serta merta, tetapi memiliki mekanisme dan syarat-syarat tertentu. Dalam konteks mekanisme, pada ayat (3) Pasal 43 tersebut disebutkan bahwa pengadaannya terlebih dahulu melalui pengusulan kepada Komite Kebijakan Industri Pertahanan (KKIP), yang notabene diketuai Presiden, untuk menggunakan produk luar negeri dengan pengadaan melalui proses langsung antarpemerintah atau kepada pabrikan. Bahkan dalam konteks kepentingan strategis nasional, DPR memberikan pertimbangan dalam pengadaan produk Alat Peralatan Pertahanan dan Keamanan tertentu sesuai dengan politik luar negeri yang dijalankan Pemerintah Pasal 43 ayat (4).

¹²⁶ ASEAN Parliamentarians for Human Rights (APHR), “Indonesia Must Halt the Import and Use of Highly Invasive Spyware from Israel and Elsewhere, Southeast Asian MPs Say,” 6 Mei 2024, <https://aseanmp.org/publications/post/indonesia-must-halt-the-import-and-use-of-highly-invasive-spyware-from-israel-and-elsewhere-southeast-asian-mps-say/>.

¹²⁷ Dalam laporannya, Amnesty Internasional menjelaskan bahwa Entitas tersebut termasuk Kepolisian Negara Republik Indonesia (Kepolisian Negara Republik Indonesia) dan Badan Siber dan Sandi Negara (Badan Siber dan Sandi Negara).

¹²⁸ APHR, “Indonesia Must Halt the Import and Use of Highly Invasive Spyware.”

¹²⁹ Amnesty International, “Unravelling a Murky Network of Spyware Exports.”

¹³⁰ Pasal 1 poin 2 UU *a quo* menjelaskan bahwa Alat Peralatan Pertahanan dan Keamanan adalah segala alat perlengkapan untuk mendukung pertahanan negara serta keamanan dan ketertiban masyarakat

Sementara pengadaan produk pertahanan-keamanan dari luar negeri tersebut, sebagaimana diatur Pasal 43 ayat (5), memiliki persyaratan yang harus dipenuhi, meliputi:

- a. Alat Peralatan Pertahanan dan Keamanan belum atau tidak bisa dibuat di dalam negeri;
- b. Mengikutsertakan Partisipasi Industri Pertahanan;
- c. Kewajiban alih teknologi;
- d. Jaminan tidak adanya potensi embargo, kondisionalitas politik dan hambatan penggunaan Alat Peralatan Pertahanan dan Keamanan dalam upaya mempertahankan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan keselamatan segenap bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara;
- e. Adanya imbal dagang, kandungan lokal dan/atau ofset paling rendah 85% (delapan puluh lima persen);
- f. Kandungan lokal dan/atau ofset sebagaimana dimaksud pada huruf e paling rendah 35% (tiga puluh lima persen) dengan peningkatan 10% (sepuluh persen) setiap 5 (lima) tahun; dan
- g. Pemberlakuan ofset paling lama 18 (delapan belas) bulan sejak Undang-Undang ini diundangkan.

Secara lebih rinci, ketentuan pengadaan alat-alat militer diatur melalui Peraturan Menteri Pertahanan No. 17 Tahun 2014 tentang Pelaksanaan Pengadaan Alat Utama Sistem Senjata di Lingkungan Kementerian Pertahanan dan Tentara Nasional Indonesia. Dalam definisinya, Pasal 1 angka 2 menjelaskan bahwa pengadaan Alutsista TNI adalah kegiatan untuk memperoleh Alutsista TNI yang pentahapannya didahului dari perencanaan kebutuhan sampai diterimanya Alutsista TNI yang berfungsi sesuai dengan peruntukannya.

Kemudian Pasal 5 ayat (1) menegaskan bahwa Pengadaan Alutsista TNI wajib menggunakan produksi dalam negeri. Namun demikian, ketentuan pada ayat (2) membuka ruang produksi luar negeri, bahwa hal Alutsista TNI sebagaimana dimaksud pada ayat (1) belum dapat dipenuhi oleh Industri Pertahanan Dalam Negeri, pengadaan produk luar negeri dapat dilaksanakan melalui proses langsung antar pemerintah atau kepada pabrikan. Hal fundamental yang patut diperhatikan adalah prinsip-prinsip pengadaan. Melalui ketentuan Pasal 8, disebutkan bahwa terdapat prinsip transparan dalam pengelolaan anggaran dan akuntabel.

Namun demikian, juga terdapat prinsip menjamin kerahasiaan yang dapat menjadi justifikasi prinsipil atas ketiadaan keterbukaan dalam pengadaan ini. Selain itu, ketentuan terhadap tim evaluasi pengadaan, sebagaimana diatur Pasal 21 juga perlu diperhatikan dengan serius. Pertama, kewenangan yang "seadanya" dalam bentuk pemberian saran dalam pelaksanaan pengadaan. Bahkan tim evaluasi pengadaan tidak perlu menandatangani Pakta Integritas. Kondisi ini perlu disoroti, karena Pakta Integritas bukan sekadar prosedur administratif, tetapi merupakan landasan normatif yang memperkuat kepercayaan publik, meningkatkan legitimasi hasil evaluasi, dan memastikan bahwa evaluasi berfungsi sebagai mekanisme akuntabilitas yang kredibel dalam tata kelola organisasi.

Kemudian, melalui Peraturan Menteri Pertahanan No. 17 Tahun 2014, dipahami bahwa terdapat tahapan pelaksanaan pengadaan alutsista TNI yang terstruktur dengan lima tahapannya, yakni:

1. Tahap pertama, yakni tahap pra-persiapan.

Tahap ini mencakup identifikasi kebutuhan alutsista berdasarkan doktrin pertahanan, rencana strategis TNI, dan analisis ancaman. Pada tahap ini, kebutuhan alutsista dirumuskan secara konseptual dan strategis, termasuk penentuan spesifikasi awal serta kesesuaiannya dengan kemampuan anggaran negara. Tahap ini krusial karena menjadi fondasi legitimasi pengadaan; kesalahan atau manipulasi pada tahap ini berpotensi melahirkan pengadaan yang tidak relevan, berlebihan, atau sarat kepentingan non-pertahanan.

2. Tahap kedua, yakni tahap persiapan

Tahap ini meliputi penyusunan dokumen pengadaan secara lebih teknis, termasuk spesifikasi final, skema pembiayaan, dan rencana pengadaan. Pada tahap ini pula dilakukan kajian kelayakan teknis dan administratif, serta penyiapan mekanisme pengadaan yang sesuai dengan peraturan perundang-undangan. Dalam konteks militerisasi teknologi, tahap persiapan seharusnya juga menjadi ruang untuk memasukkan pertimbangan risiko jangka panjang, termasuk ketergantungan teknologi, keamanan data, dan potensi dampak terhadap HAM, meskipun aspek ini belum diatur secara eksplisit dalam Permenhan tersebut.

3. Tahap ketiga, yakni tahap pemilihan penyedia alutsista TNI

Tahap ini merupakan fase paling sensitif dari sisi integritas dan potensi pelanggaran hukum. Tahap ini mencakup proses seleksi, evaluasi, dan penetapan penyedia barang atau jasa pertahanan, baik dari dalam negeri maupun luar negeri. Mengingat karakter alutsista yang strategis dan sering kali diklasifikasikan, tahap ini kerap dilakukan dengan mekanisme khusus. Namun demikian, tanpa pengawasan yang memadai, fase ini rawan terhadap praktik korupsi, konflik kepentingan, dan pengabaian prinsip *value for money*.

4. Tahap keempat, yakni tahap penyusunan dan aktifasi kontrak

Tahap ini merupakan tahap ketika hubungan hukum antara negara dan penyedia alutsista diformalkan. Kontrak mencakup ruang lingkup pekerjaan, kewajiban para pihak, jangka waktu, serta mekanisme penyelesaian sengketa. Dalam pengadaan teknologi militer modern, kontrak juga seharusnya mengatur aspek transfer teknologi, perlindungan data, dan tanggung jawab atas kegagalan sistem. Kelemahan dalam tahap ini dapat berdampak panjang, terutama jika kontrak tidak cukup melindungi kepentingan negara atau membuka celah ketergantungan strategis pada pihak asing.

5. Tahap kelima, yakni tahapan pelaksanaan dan penyerahan hasil pekerjaan

Tahap ini mencakup proses produksi, pengiriman, pengujian, serta serah terima alutsista kepada TNI. Tahap ini juga menjadi momen penting untuk memastikan bahwa alutsista yang diterima sesuai dengan spesifikasi, berfungsi dengan baik, dan siap dioperasikan. Dari perspektif akuntabilitas, tahap ini menuntut mekanisme

pengawasan dan evaluasi yang kuat, karena kegagalan atau penyimpangan di fase ini dapat berimplikasi langsung pada efektivitas pertahanan dan pemborosan anggaran negara.

Secara keseluruhan, Permenhan No. 17 Tahun 2014 menunjukkan bahwa pengadaan alutsista TNI telah dirancang melalui tahapan yang sistematis dan berlapis. Namun, dalam konteks kontemporer militerisasi teknologi—terutama teknologi digital, siber, dan *surveillance*—regulasi ini masih cenderung berorientasi pada aspek prosedural dan administratif, belum secara eksplisit memasukkan dimensi perlindungan HAM, transparansi publik, dan penilaian risiko sosial. Oleh karena itu, penguatan regulasi turunan dan integrasi prinsip HAM serta akuntabilitas demokratis menjadi agenda penting agar pengadaan alutsista tidak hanya sah secara prosedural, tetapi juga legitimate secara hukum dan etika publik.

4.3. Bagaimana model pertanggungjawabannya dapat dikerangkakan?

Perkembangan pesat teknologi digital—seperti kecerdasan buatan (AI), sistem pengawasan (*surveillance*), teknologi siber, drone (UAV), dan alat intelijen digital—telah mengubah lanskap pertahanan dan keamanan Indonesia. Di satu sisi, teknologi ini dipandang penting untuk menghadapi ancaman non-tradisional dan kompleks. Namun, di sisi lain, militerisasi teknologi yang tidak diiringi mekanisme akuntabilitas, transparansi, dan perlindungan HAM berpotensi menimbulkan pelanggaran serius terhadap hak privasi, kebebasan berekspresi, dan prinsip kontrol sipil atas militer.

Gambar 10 Pengaturan Teknologi Agar Tetap Etis



Sumber: <https://widya.ai/>

Perlu hadir model pertanggungjawabannya yang dapat dikerangkakan untuk memastikan bahwa militerisasi teknologi di Indonesia tetap berada dalam koridor negara hukum demokratis dan penghormatan HAM, dengan menekankan pentingnya pengawasan sipil, akuntabilitas anggaran, serta regulasi berbasis risiko. Dalam konteks pondasi utama, militerisasi teknologi perlu dipastikan kepatuhan terhadap berbagai ketentuan perundang-undangan yang menjamin hak-hak warga negara, seperti UUD NRI 1945, UU No. 39 Tahun 1999 tentang HAM, UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta berbagai instrumen internasional yang berkaitan dengan Hukum Humaniter Internasional dan HAM internasional.

Kepatuhan tersebut diperkuat dan/atau juga diwujudkan melalui sistem, seperti dalam aspek pengawasan dan akuntabilitas: (1) penguatan fungsi pengawasan oleh lembaga legislatif, tepatnya pengawasan substantif, bukan sekedar formalitas; (2) memastikan pengawasan berlapis dengan melibatkan lembaga-lembaga seperti Komnas HAM dan Ombudsman RI, serta menyiapkan mekanisme preventif untuk mengantisipasi pelanggaran maupun mekanisme pengaduan publik yang responsif pasca-terjadi pelanggaran; (3) melakukan pengategorian, seperti Korea Selatan, terhadap informasi-informasi yang dapat diakses publik, baik dalam dokumen anggaran dan laporan pengadaan teknologi.

Aspek regulasi dan *complaint mechanism* juga perlu menjadi penekanan, seperti (1) sebagai bagian dari konstruksi negara hukum dan memastikan kepastian hukum, maka pengadaan dan penggunaan teknologi harus memiliki dasar hukum eksplisit, bukan hanya kebijakan internal militer; (2) izin penggunaan teknologi tertentu (*spyware*, *AI surveillance*) harus diberikan sebelum digunakan, bukan setelah pelanggaran terjadi; serta (3) warga harus memiliki akses menggugat penyalahgunaan teknologi (misalnya *surveillance illegal*).

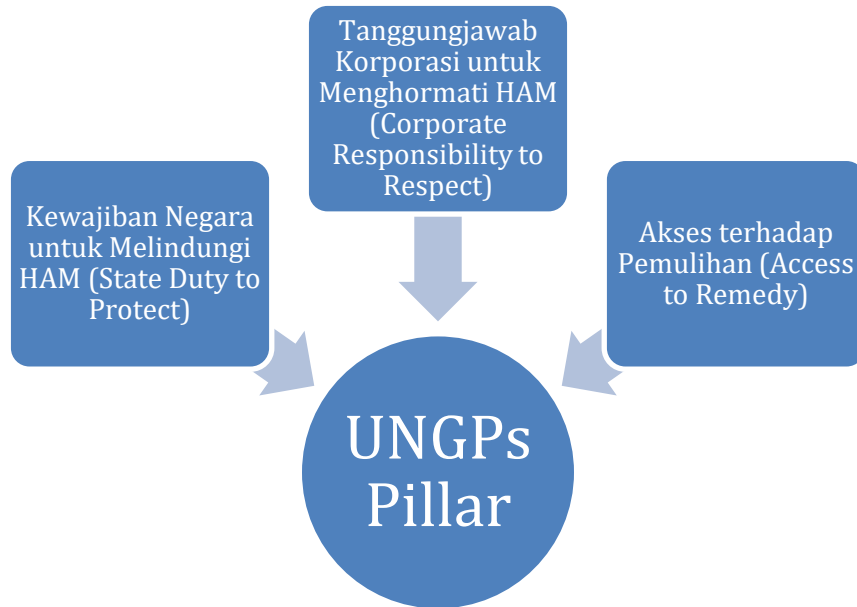
Salah satu poin mendasar dalam desain pengaturan tersebut dapat mengacu kepada penelitian Arifianto (2005), yang menegaskan bahwa tidak perlu ada perlakuan khusus atas pengelolaan anggaran belanja militer (Dephan-TNI) secara menyeluruh. Perlakuan khusus harus ditetapkan secara terbatas pada hal-hal yang bersifat kontijensi dan rahasia seperti kegiatan operasi militer yang mendesak atau mendadak dengan memperbaiki sistem pengendalian internal dan sistem pertanggungjawaban keuangan yang lebih transparan dan akuntabel dalam rangka mewujudkan tata kelola pemerintahan yang baik dalam pengelolaan keuangan negara.¹³¹

Berbagai penjelasan sebelumnya, memperlihatkan bahwa dalam konteks militerisasi teknologi ini negara semakin kerap menjalin kemitraan dengan aktor swasta, baik sebagai penyedia teknologi, pengembang sistem, maupun operator pendukung. Pola ini menciptakan perluasan aktor yang terlibat dalam praktik-praktik yang berpotensi membatasi atau melanggar hak asasi manusia, terutama hak atas privasi, kebebasan berekspresi, dan perlindungan dari pengawasan sewenang-wenang. Dalam situasi demikian, penerapan Uji Tuntas HAM (*human rights due diligence/ HRDD*) sebagaimana

¹³¹ Arifianto, *Sistem Pengelolaan Anggaran Belanja Militer di Indonesia*.

ditegaskan dalam *United Nations Guiding Principles on Business and Human Rights* (UNGPs) menjadi penting.

Kepatuhan terhadap UNGPs, dapat menekan perusahaan untuk mengadopsi 3 (tiga) pilar utama UNGPs, yakni:



Adopsi uji tuntas HAM dalam kemitraan militer–swasta memungkinkan identifikasi, pencegahan, dan mitigasi risiko HAM sejak tahap perencanaan, pengadaan, hingga penggunaan teknologi militer. Dengan demikian, HRDD tidak hanya berfungsi sebagai instrumen etis, tetapi juga sebagai mekanisme konkret untuk memastikan bahwa militerisasi teknologi tetap berada dalam kerangka akuntabilitas demokratis, supremasi hukum, dan penghormatan terhadap hak asasi manusia, sekalipun dijalankan melalui relasi kompleks antara negara dan sektor swasta.

Prinsip UNGPs juga perlu dikembangkan agar memiliki perspektif berbasis gender. Misalnya mekanisme akuntabilitas harus menjamin partisipasi bermakna perempuan dan organisasi masyarakat sipil berbasis gender dalam proses pengawasan, evaluasi, dan penyusunan kebijakan keamanan digital. Transparansi terbatas yang selama ini dibenarkan atas nama pertahanan dan keamanan negara perlu diimbangi dengan pengungkapan informasi yang cukup untuk menilai risiko HAM, termasuk risiko kekerasan dan diskriminasi berbasis gender. Selain itu, akses terhadap mekanisme pengaduan dan pemulihan (*access to remedy*) harus dirancang aman, inklusif, dan responsif terhadap pengalaman korban perempuan, baik dalam ranah administratif, yudisial, maupun non-yudisial.

Selain itu, prinsip dasar dalam Hukum Humaniter Internasional (*Internasional Humanitarian Law/IHL*) yang menjadi acuan dalam pembatasan metode dan sarana

dalam peperangan, juga perlu menjadi acuan dalam pengaturan teknologi militer yang beririsan dengan HAM. Terdapat empat prinsip dasar yang dimaksud, yakni:¹³²

1. Perbedaan (*distinction*): harus ada perbedaan yang jelas antara angkatan bersenjata dan warga sipil, dan antara objek yang mungkin diserang secara sah dan objek yang dilindungi dari serangan
2. Keperluan militer (*military necessity*): pihak yang terlibat dalam konflik bersenjata hanya boleh menggunakan kekuatan dalam tingkat dan jenis yang tidak dilarang oleh hukum konflik bersenjata, yang diperlukan untuk mencapai tujuan sah dari konflik tersebut, yaitu penaklukan musuh secara keseluruhan atau sebagian secepat mungkin dengan pengeluaran sumber daya yang seminimal mungkin.
3. Kemanusiaan (*humanity*): kemanusiaan melarang penimbunan penderitaan, cedera, atau kerusakan yang sebenarnya tidak diperlukan untuk tercapainya tujuan militer yang sah
4. Proporsionalitas (*proportionality*): kerugian yang diakibatkan oleh suatu tindakan militer tidak boleh terlalu besar dibandingkan dengan keuntungan militer yang diharapkan.

Hukum humaniter internasional menegaskan prinsip perbedaan (*distinction*), yang mewajibkan pihak-pihak yang berkonflik untuk membedakan objek sipil dari sasaran militer yang sah. Kondisi ini mengharuskan keberadaan prosedur verifikasi berlapis sebelum penetapan target digital, serta kewajiban *human-in-the-loop*, yakni manusia tetap memutuskan serangan. Kemudian dengan prinsip keperluan, dapat dibatasi penggunaan kekuatan atau teknologi yang tidak diperlukan untuk mencapai tujuan militer yang sah.

Penguatan pengaturan terhadap militerisasi teknologi juga dapat mengadopsi *NATO's AI governance* mengenai Prinsip Penggunaan yang Bertanggung Jawab (*Principles of Responsible Use/PRUs*) untuk aplikasi militer. Terdapat enam prinsip yang diperbarui pada tahun 2024, yang bertujuan memastikan bahwa AI digunakan secara aman dan etis dalam batasan hukum internasional dan nilai-nilai demokrasi, yakni:¹³³

1. Keabsahan (*Lawfulness*): Penggunaan AI harus mematuhi hukum nasional dan internasional, termasuk hukum humaniter internasional.
2. Tanggung Jawab dan Akuntabilitas (*Responsibility and Accountability*): Tanggung jawab manusia harus dijaga, dan akuntabilitas tidak dapat dialihkan ke mesin.
3. Dapat Dijelaskan dan Ditelusuri (*Explainability and Traceability*): AI harus dapat dipahami dan transparan, dengan mekanisme peninjauan dan validasi yang tepat.
4. Keandalan (*Reliability*): AI ditujukan untuk kasus penggunaan tertentu, dengan keselamatan dan keamanan yang diuji sepanjang siklus hidupnya

¹³² Foreign & Commonwealth Office dan Foreign, Commonwealth & Development Office, "The UK and International Humanitarian Law," GOV.UK, 24 Juli 2018, diperbarui 4 April 2024, <https://www.gov.uk/government/publications/international-humanitarian-law-and-the-uk-government/uk-and-international-humanitarian-law-2018>.

¹³³ NATO, *Summary of NATO's Revised Artificial Intelligence (AI) Strategy*, 10 Juli 2024, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy>.

5. Tata Kelola (*Governability*): Desain AI harus memungkinkan interaksi manusia, mendeteksi konsekuensi yang tidak diinginkan, dan memiliki kapasitas untuk menonaktifkan.
6. Mitigasi Bias (*Bias Mitigation*): Langkah-langkah harus diambil untuk meminimalkan bias yang tidak diinginkan dalam pengembangan AI, penggunaan, dan data pelatihan.

Pengaturan dan pembatasan terhadap militerisasi teknologi ini sejalan dengan Undang-Undang AI Uni Eropa (*EU Artificial Intelligence Act*), *article 5: Prohibited AI Practices*, yang menegaskan larangan penggunaan kecerdasan buatan (AI) tertentu. Ini termasuk sistem AI yang memanipulasi keputusan manusia atau mengeksploitasi kerentanan mereka, sistem yang mengevaluasi atau mengklasifikasikan orang berdasarkan perilaku sosial atau ciri-ciri pribadi mereka, dan sistem yang memprediksi risiko seseorang melakukan kejahatan.¹³⁴

Undang-Undang ini juga melarang sistem AI yang mengambil gambar wajah dari internet atau rekaman CCTV, menyimpulkan emosi di tempat kerja atau institusi pendidikan, dan mengkategorikan orang berdasarkan data biometrik mereka. Namun, beberapa pengecualian dibuat untuk tujuan penegakan hukum, seperti mencari orang hilang atau mencegah serangan teroris.¹³⁵

Pengalaman Uni Eropa melalui *EU Artificial Intelligence Act*, khususnya Article 5 tentang *Prohibited AI Practices*, memberikan standar normatif penting mengenai batas-batas penggunaan teknologi berisiko tinggi. Aturan tersebut menegaskan bahwa inovasi teknologi tidak boleh mengabaikan martabat manusia, privasi, dan prinsip-prinsip demokrasi. Dengan melarang praktik seperti manipulasi perilaku melalui AI, prediksi risiko kriminal berdasarkan karakteristik personal, penggunaan identifikasi biometrik masif dari CCTV atau gambar daring, dan inferensi emosional di ruang kerja atau pendidikan, Uni Eropa memperlihatkan bahwa batasan teknologis dapat diatur secara tegas tanpa menghambat tujuan keamanan kolektif.

Dalam konteks Indonesia, prinsip-prinsip ini memberikan landasan penting bahwa militerisasi teknologi harus dipandu oleh norma HAM universal, prinsip negara hukum, dan kontrol sipil yang demokratis. Penggunaan teknologi oleh militer tidak boleh diperluas tanpa batas atau tanpa evaluasi, terutama ketika melibatkan pemantauan massal, pengumpulan data biometrik, atau analitik prediktif yang berpotensi mengkriminalkan kelompok tertentu. Sementara pengecualian untuk tujuan penegakan hukum—seperti pencarian orang hilang atau pencegahan tindakan terorisme—adalah wajar, praktik tersebut tetap harus berada di bawah mekanisme pengawasan ketat, izin yudisial, dan evaluasi HAM yang terukur.

Oleh karena itu, Indonesia perlu mengembangkan kerangka regulatif yang sejalan dengan standar internasional, dengan mengadopsi prinsip-prinsip dasar dari EU AI Act: *prohibition of harmful AI*, *risk-based governance*, dan *democratic accountability*.

¹³⁴ “Article 5: Prohibited AI Practices,” *ArtificialIntelligenceAct.eu*, <https://artificialintelligenceact.eu/article/5/article-5-prohibited-ai-practices>, diakses 2 Desember 2025

¹³⁵ “Article 5: Prohibited AI Practices.”

Pengaturan tersebut harus mencakup batasan substantif atas penggunaan teknologi berisiko tinggi, mekanisme evaluasi independen, serta kontrol sipil terhadap proses pengadaan dan implementasi teknologi militer. Agar model pertanggungjawaban dapat memiliki kekuatan hukum yang kuat, maka tingkat Undang-Undang dapat menjadi opsi utama.

4.4. Melihat Pengaturan Terkait dengan Militerisasi Teknologi di Indonesia

Dalam konteks militerisasi teknologi, maka peta permasalahan dapat dibagi 5 (lima), meliputi: (1) Ketidadaan regulasi khusus yang mengatur penggunaan teknologi militer digital, khususnya teknologi surveillance dan AI; (2) Dalih kerahasiaan pertahanan sering digunakan untuk membatasi transparansi anggaran dan informasi publik (UU KIP Pasal 17); (3) Pengawasan parlemen terbatas dan asimetris, terutama dalam pengadaan alat intelijen dan sistem siber; (4) Minimnya penilaian dampak HAM sebelum pengadaan dan penggunaan teknologi pertahanan; dan (5) Risiko normalisasi pengawasan massal, terutama di ruang siber dan terhadap warga sipil.

Meskipun belum ada regulasi yang spesifik mengaturnya, dalam konteks kerangka regulasi, di Indonesia sesungguhnya telah memiliki beberapa instrumen hukum yang relevan untuk memastikan demokratisasi teknologi, meskipun belum dirancang secara spesifik untuk mengatur dampak teknologi militer terhadap HAM dan tata kelola demokratis.

Secara prinsipil, pengaturan tersebut terdapat dalam Konstitusi, khususnya Pasal 28D berupa hak atas pengakuan, jaminan, perlindungan, kepastian hukum yang adil, serta perlakuan yang sama di depan hukum. Kemudian juga Pasal 28G yang mengatur Hak perlindungan diri pribadi, keluarga, kehormatan, martabat, harta benda, dan rasa aman. Hal-hal prinsipil ini kemudian diperkuat melalui UU No. 39 Tahun 1999 tentang Hak Asasi Manusia.

Berbagai instrumen HAM internasional yang telah diratifikasi Indonesia juga dapat menjadi penguat dalam pengaturan militerisasi teknologi ini, meliputi:

1. *International Covenant on Civil and Political Rights* (ICCPR) atau Kovenan Internasional tentang Hak-Hak Sipil dan Politik. Instrumen ini merupakan dasar utama pembatasan penggunaan teknologi surveillance oleh negara. ICCPR menjamin: hak atas privasi (*Right to privacy*), kebebasan berekspresi (*Freedom of expression*), kebebasan berkumpul dan berserikat (*Freedom of assembly and association*). Setiap pembatasan atas hak-hak tersebut, termasuk melalui teknologi militer atau intelijen digital, harus memenuhi prinsip *legality*, *necessity*, dan *proportionality*. ICCPR sangat relevan untuk menilai penggunaan surveillance militer di ruang sipil dan operasi keamanan domestik. Instrumen ini telah diratifikasi melalui UU No. 12 Tahun 2005 Tentang Pengesahan *International Covenant on Civil and Political Rights* (Kovenan Internasional Tentang Hak-Hak Sipil dan Politik).
2. *International Covenant on Economic, Social and Cultural Rights* (ICESCR) atau Kovenan Internasional tentang Hak-Hak Ekonomi, Sosial, dan Budaya. Meskipun tidak secara langsung mengatur surveillance, ICESCR penting dalam konteks prioritas anggaran negara. Militerisasi teknologi yang menyerap anggaran besar

berpotensi mengurangi pemenuhan hak atas Pendidikan, Kesehatan, dan kesejahteraan sosial. Instrumen ini memperkuat argumen bahwa belanja teknologi militer harus tunduk pada prinsip *maximum available resources* dan akuntabilitas fiskal. Instrumen ini telah diratifikasi melalui UU No. 11 Tahun 2005 tentang *Pengesahan International Covenant on Economic, Social and Cultural Rights* (Kovenan Internasional tentang Hak-Hak Ekonomi, Sosial dan Budaya).

3. *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment* (CAT) atau Konvensi Menentang Penyiksaan dan Perlakuan atau Hukuman Lain yang Kejam, Tidak Manusiawi, atau Merendahkan Martabat. Instrumen CAT ini relevan ketika teknologi *surveillance* digunakan untuk profiling, penargetan individu, atau operasi intelijen yang berujung pada penahanan sewenang-wenang. Sebab Penggunaan teknologi untuk mendukung praktik represif dapat menimbulkan tanggung jawab negara, termasuk jika teknologi tersebut memfasilitasi penyiksaan atau perlakuan tidak manusiawi. Instrumen ini telah diratifikasi melalui UU No. 5 Tahun 1998 tentang pengesahan Konvensi Menentang Penyiksaan dan Perlakuan atau Penghukuman Lain yang Kejam, Tidak Manusiawi, atau Merendahkan Martabat Manusia (*Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*).
4. *Convention on the Rights of the Child* (CRC) atau Konvensi Hak Anak. Instrumen CRC dapat memperkuat pembatasan penggunaan teknologi *surveillance* terhadap anak-anak, pelajar, dan ruang pendidikan. Teknologi pengawasan berbasis biometrik, pemantauan digital, atau pengumpulan data anak oleh aparat negara harus tunduk pada prinsip *best interests of the child* dan perlindungan privasi anak. Instrumen ini telah diratifikasi melalui Keputusan Presiden (Keppres) No. 36 Tahun 1990 yang mengesahkan (meratifikasi) “Convention on the Rights of the Child” atau Konvensi Hak-Hak Anak PBB.
5. *Convention on the Elimination of All Forms of Discrimination against Women* (CEDAW) atau Konvensi tentang Penghapusan Segala Bentuk Diskriminasi terhadap Perempuan. Instrumen CEDAW relevan dalam konteks risiko *gendered surveillance*, ketika teknologi keamanan dapat digunakan secara diskriminatif terhadap perempuan, aktivis, atau kelompok rentan. Instrumen ini memperkuat kewajiban negara untuk memastikan bahwa teknologi militer tidak memperdalam ketimpangan dan diskriminasi. Instrumen ini diratifikasi melalui UU No. 7 Tahun 1984 tentang Pengesahan Konvensi Mengenai Penghapusan Segala Bentuk Diskriminasi Terhadap Wanita (*Convention on the Elimination of All Forms of Discrimination Against Women* - CEDAW).

Penguatan terhadap prinsip-prinsip HAM dan jaminan Konstitusi tersebut terlihat melalui keberadaan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang berorientasi pada perlindungan hak warga negara, terutama data pribadi. Terdapat 2 (dua) poin penting dalam konsideransnya, yakni:

- a. Pelindungan data pribadi merupakan salah satu hak asasi manusia yang merupakan bagian dari pelindungan diri pribadi maka perlu diberikan landasan

hukum untuk memberikan keamanan atas data pribadi, berdasarkan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

- b. Pelindungan data pribadi ditujukan untuk menjamin hak warga negara atas pelindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya pelindungan data pribadi;

UU PDP memberikan fondasi normatif penting dalam membatasi penggunaan teknologi berbasis data, termasuk teknologi pengawasan, biometrik, dan sistem kecerdasan buatan yang lazim digunakan dalam sektor pertahanan dan intelijen. Sebab terdapat penegasan bahwa pengendali data pribadi,¹³⁶ sebagaimana Pasal 38, wajib melindungi Data Pribadi dari pemrosesan yang tidak sah.

Selain itu, UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya (UU No. 19 Tahun 2016 dan UU No. 1 Tahun 2024) dalam konteks penguatan pengaturan militerisasi teknologi, juga memuat sejumlah ketentuan yang secara implisit melindungi hak-hak sipil digital, sehingga dapat berfungsi sebagai instrumen domestik pendukung (*supporting legal framework*) dalam mengendalikan dampak militerisasi teknologi, terutama di ruang siber. Misalnya Pasal 30 UU ITE yang mengatur larangan akses tanpa hak terhadap sistem elektronik milik orang lain, Pasal 32 UU ITE melarang perusakan, pengubahan, atau pemindahan data elektronik tanpa hak.¹³⁷

Berbagai regulasi di atas menegaskan kewajiban negara untuk melindungi hak-hak dasar individu dari segala bentuk penyalahgunaan kekuasaan, termasuk yang dimediasi oleh perkembangan teknologi. Dalam konteks militerisasi teknologi dan penggunaan sistem *surveillance* oleh pemerintah melalui aparat negara, Konstitusi dan UU HAM memberikan landasan normatif bahwa hak atas privasi, kebebasan berpendapat, berekspresi, dan rasa aman merupakan hak yang melekat pada setiap individu dan tidak dapat dikurangi secara sewenang-wenang. Negara, termasuk institusi militer dan keamanan, terikat pada prinsip penghormatan, perlindungan, dan pemenuhan HAM dalam setiap kebijakan dan tindakan, terlepas dari dalih keamanan nasional.

5. Penggunaan Teknologi Dwiguna dalam Konteks Modernisasi Militer Indonesia dan Dampaknya Terhadap HAM

Konteks dan Relevansi

Pengeluaran militer sering kali mendapatkan justifikasi dengan alasan pencegahan dan keamanan nasional. Namun, bukti menunjukkan peningkatan pengeluaran militer tidak selalu mengarah pada perdamaian atau stabilitas yang lebih besar. Sebaliknya, hal itu sering memperburuk ketegangan geopolitik, memicu perlombaan senjata, dan

¹³⁶ Dalam UU a quo, Pasal 1 angka 4 mendefinisikan Pengendali Data Pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan Data Pribadi.

¹³⁷ Namun demikian, juga terdapat catatan terhadap UU ITE, seperti potensi perluasan kewenangan negara dalam pengaturan, pengawasan, dan penegakan hukum berbasis teknologi, serta belum secara eksplisit membatasi tindakan aparat negara, terutama jika dikaitkan dengan alasan keamanan nasional.

meningkatkan risiko konflik, terutama ketika dikaitkan dengan tata pemerintahan yang lemah, meningkatnya ketidaksetaraan, dan ketidakpercayaan sistemik. Meningkatnya pengeluaran militer saat ini menggeser sumber daya yang penting untuk investasi sosial, pengurangan kemiskinan, pendidikan, kesehatan, perlindungan lingkungan, dan infrastruktur – merusak kemajuan di hampir semua Tujuan Pembangunan Berkelanjutan (*Sustainable Development Goals*).¹³⁸

Sementara itu, pengeluaran militer global telah meningkat dengan laju rekor selama satu dekade sebagai respons terhadap memburuknya lingkungan keamanan global.¹³⁹ Menurut data baru yang diterbitkan oleh Stockholm International Peace Research Institute (SIPRI) pengeluaran militer dunia mencapai \$2.887 miliar pada tahun 2025, meningkat 2,9 persen secara riil dibandingkan tahun 2024. Pengeluaran militer menurun di Amerika Serikat tetapi meningkat sebesar 14 persen di Eropa dan sebesar 8,1 persen di Asia dan Oseania. Tiga negara dengan pengeluaran militer terbesar, Amerika Serikat, Tiongkok, dan Rusia menghabiskan total gabungan sebesar \$1.480 miliar, atau 51 persen dari total global. Pengeluaran militer global kembali meningkat pada 2025 karena negara-negara menanggapi tahun lain yang penuh perang, ketidakpastian, dan gejolak geopolitik dengan peningkatan persenjataan skala besar.¹⁴⁰ Pemerintah dan perusahaan di seluruh dunia berlomba-lomba untuk membangun dominasi dan menjerumuskan pengguna teknologi ke dalam perlombaan teknologi. Perlombaan teknologi telah mendefinisikan ulang medan pertempuran dan mengaburkan batas antara infrastruktur sipil dan militer. Pergeseran dramatis ini memengaruhi segala sisi kehidupan setiap individu dan membentuk kembali masa depan kemanusiaan dan secara radikal mengubah prioritas politik dan investasi.¹⁴¹ Pemerintah dengan cepat memiliterisasi masyarakat dengan strategi politik meningkatkan pengeluaran militer yang berimplikasi melemahkan perlindungan hak-hak sipil, dan mengurangi program perlindungan sosial. Era globalisasi ditandai pemerintah semakin bergantung pada sektor swasta untuk menyediakan layanan publik, melalui kemitraan publik-swasta (*public-private partnerships*).¹⁴²

¹³⁸ United Nations. Secretary-General, *The Security We Need: Rebalancing Military Spending for a Sustainable and Peaceful Future: Report of the Secretary-General on the Impact of the Global Increase in Military Expenditure on the Achievement of the Sustainable Development Goals as Requested by Action 13(c) of the Pact for the Future* (2025), https://digitallibrary.un.org/record/4088022/files/SG_Report_TheSecurityWeNeed.pdf.

¹³⁹ Nan Tian dan Xiao Liang, *Rebalancing Military Spending Towards Achieving Sustainable Development*, SIPRI Research Policy Paper (Stockholm: Stockholm International Peace Research Institute [SIPRI], November 2025), <https://doi.org/10.55163/ZCIE5196>.

¹⁴⁰ SIPRI, "Global Military Spending Rise Continues."

¹⁴¹ Privacy International, "Challenging the Militarisation of Tech," <https://privacyinternational.org/campaigns/militarisation-of-tech>.

¹⁴² Privacy International, "What Is Militarisation of Tech?," 12 September 2025, <https://privacyinternational.org/long-read/5668/what-militarisation-tech>.

Platform digital besar Meta (Facebook), Amazon, Microsoft, Alphabet (Google), dan Apple, yang sering disebut perusahaan Big Tech kini mendominasi ekonomi dunia. Kapitalisasi pasar Big Tech telah melampaui Produk Domestik Bruto negara-negara dengan perekonomian besar, seperti Jerman atau Jepang. Bahkan Big Tech juga telah mengendalikan sebagian besar penelitian dan pengembangan global dan paten yang terkait dengan teknologi mutakhir, seperti kecerdasan artifisial. Fakta-fakta ini ini mencerminkan konsentrasi kekuatan tekno-ekonomi yang belum pernah terjadi sebelumnya, dengan implikasi besar terhadap distribusi pendapatan, akses terhadap pengetahuan dan inovasi, fragmentasi dan prekarisasi tenaga kerja, serta meningkatnya ketegangan geopolitik. Inti dari kekuatan perusahaan-perusahaan Big Tech termanifestasi pada kendali atas pengetahuan, infrastruktur, misalnya pusat data, kabel bawah laut, dan teknologi dwiguna (*dual-use technologies*), yaitu komputasi awan, kecerdasan artifisial, dan sistem navigasi dan komunikasi satelit baru yang sangat penting baik di bidang sipil maupun militer.¹⁴³

Pada saat bersamaan, selama dekade terakhir, pusat kompleks industri militer Amerika perlahan bergeser dari kawasan Washington D.C. ke Silicon Valley. Meskipun sebagian besar anggaran Pentagon sebesar \$886 miliar dihabiskan untuk sistem senjata konvensional,¹⁴⁴ namun ekonomi politik baru sedang muncul yang didorong oleh perusahaan teknologi besar, modal ventura, dan perusahaan ekuitas swasta yang menopang industri militer. Ketika para pejabat Departemen Pertahanan Amerika Serikat berupaya mengadopsi sistem yang didukung kecerdasan artifisial dan layanan komputasi awan yang aman, Departemen Pertahanan telah memberikan kontrak besar senilai miliaran dolar kepada Microsoft, Amazon, Google, dan Oracle. Pada saat yang sama, Pentagon telah meningkatkan pendanaan untuk perusahaan rintisan teknologi pertahanan yang lebih kecil yang berupaya untuk mengganggu pasar yang ada (*to disrupt existing markets*) dan bergerak cepat dan merusak sesuatu (*move fast and break things*).¹⁴⁵

Sama dua tahun terakhir, peristiwa global semakin memicu permintaan Pentagon akan teknologi Silicon Valley, termasuk pengerahan drone dan sistem senjata berbasis kecerdasan artifisial di Ukraina dan Gaza, serta kekhawatiran akan perlombaan senjata kecerdasan artifisial global melawan Cina. Prospek perang siber dan kampanye disinformasi Rusia juga telah memotivasi para pejabat Departemen Pertahanan untuk

¹⁴³ Andrea Coveri, Claudio Cozza, dan Dario Guarascio, "Big Tech and the US Digital-Military-Industrial Complex," *Intereconomics* 60, no. 2 (2025): 81–87, <https://doi.org/10.2478/ie-2025-0017>.

¹⁴⁴ Anggaran tersebut disalurkan kepada raksasa pertahanan yang sudah mapan seperti Lockheed Martin, RTX, Northrop Grumman, General Dynamics, Boeing, dan BAE Systems. Lihat Roberto J. González, *How Big Tech and Silicon Valley Are Transforming the Military-Industrial Complex* (Costs of War, Watson Institute for International and Public Affairs, Brown University, 17 April 2024), <https://costsofwar.watson.brown.edu/paper/how-big-tech-and-silicon-valley-are-transforming-military-industrial-complex>.

¹⁴⁵ González, *How Big Tech and Silicon Valley Are Transforming the Military-Industrial Complex*.

berinvestasi besar-besaran dalam teknologi digital baru. Hal ini memicu para pejabat Departemen Pertahanan Amerika Serikat menguraikan rencana untuk mengembangkan armada drone udara, maritim, dan darat otonom yang luas untuk transportasi, surveilans, dan pertempuran; memperoleh kemampuan komputasi awan komersial untuk berbagi data, penyimpanan data, dan konektivitas tanpa batas. Teknologi digital baru ini akan memperkuat sistem pertahanan siber Amerika Serikat dan menggunakan kecerdasan artifisial untuk pelatihan dan latihan simulasi pertempuran.¹⁴⁶

Situasi ini menempatkan perusahaan-perusahaan Big Tech kini menjadi pemain kunci dalam benturan antara dua kompleks industri-militer-digital (*digital-military-industrial complexes*) yang bersaing untuk meraih hegemoni global. Persaingan ini berkontribusi pada semakin kaburnya batas antara negara dan korporasi dibandingkan dengan yang situasi pada paruh kedua abad ke-20 dengan munculnya korporasi transnasional. Dalam hal ini, peran Elon Musk dalam Pemerintahan Donald Trump dan loyalitas yang ditunjukkan oleh para CEO Big Tech lainnya selama upacara pelantikan mendukung hipotesis konvergensi kepentingan strategis dalam pengembangan militer dalam teknologi.¹⁴⁷

Saat ini, aparat militer dan intelijen tidak dapat berfungsi tanpa Big Tech. Perusahaan-perusahaan ini mengendalikan perangkat digital, di antaranya, sistem cloud atau algoritma kecerdasan artifisial yang ditujukan untuk pengenalan gambar dan suara, prediksi perilaku, dan penargetan militer yang penting untuk memata-matai musuh dan sekutu dan untuk mengantisipasi gerakan mereka di medan perang. Perusahaan-perusahaan ini memainkan peran penting dalam ekosistem inovasi terkait militer, membantu memobilisasi upaya penelitian dan pengembangan dari perusahaan rintisan dan memfasilitasi transfer teknologi yang dirancang untuk domain sipil ke bidang militer. Lebih jauh, platform media yang dijalankan oleh Big Tech, misalnya, Platform media sosial X, yang dimiliki oleh Elon Musk, mendukung pembangunan konsensus politik dan memengaruhi opini publik, baik di dalam maupun luar negeri.¹⁴⁸

Pada saat bersamaan dalam beberapa tahun terakhir pengeluaran modal ventura (*venture capital*) untuk teknologi pertahanan mencapai rekor tertinggi pada 2025, dengan perusahaan rintisan pertahanan (*Defense-Tech Start-Ups*) yang didukung oleh modal ventura di Amerika Serikat dan Eropa. Beberapa prediksi mengkalkulasi dukungan modal ventura terhadap perusahaan rintisan teknologi pertahanan mencapai total \$7,7 miliar antara Januari dan Oktober 2025, lebih dari dua kali lipat total tahun 2024. Secara keseluruhan, investasi pertahanan swasta pada tahun 2025 melebihi \$48 miliar, didorong oleh putaran pendanaan besar untuk perusahaan di sektor kecerdasan artifisial dan

¹⁴⁶ González, *How Big Tech and Silicon Valley Are Transforming the Military-Industrial Complex*.

¹⁴⁷ Coveri, Cozza, dan Guarascio, "Big Tech and the US Digital-Military-Industrial Complex."

¹⁴⁸ Coveri, Cozza, dan Guarascio, "Big Tech and the US Digital-Military-Industrial Complex."

drone otonom. Minat yang meningkat ini sebagian besar merupakan hasil dari janji pengeluaran pemerintah yang tinggi untuk pertahanan dan meningkatnya minat pada kegunaan kecerdasan artifisial di medan perang.¹⁴⁹

Selain pengeluaran militer global yang cenderung terus melonjak selama dekade terakhir, jangkauan teknologi militer juga meluas, dengan garis batas antara instrumen perang dan perdamaian menjadi semakin kabur. Inggris, Eropa, dan Amerika Serikat memanfaatkan teknologi yang dikembangkan di medan perang untuk memantau warga dan mengawasi pengungsi di perbatasan mereka. Raksasa senjata menjadi penyedia teknologi utama bagi polisi, badan perbatasan, dan badan publik lainnya.¹⁵⁰ Saat ini, teknologi dwiguna mencakup berbagai industri dan bidang teknologi, termasuk kecerdasan artifisial, material canggih (*advanced materials*), nanoteknologi, perangkat keamanan siber, teknologi satelit, bioteknologi, kuantum, kedirgantaraan, dan drone. Teknologi dwiguna bukan hanya strategi pertahanan dan komersial karena merupakan strategi bisnis bagi perusahaan inovatif. Perusahaan yang mengembangkan dan mengkomersialkan teknologi dwiguna harus mengelola dua pelanggan dan rantai nilai yang seringkali berbeda. Meskipun ada manfaat memiliki berbagai pelanggan dari pembeli pemerintah dan komersial.¹⁵¹

Invasi skala penuh Rusia ke Ukraina pada 2022 telah menjadi faktor utama di balik kebangkitan kembali minat pada teknologi dwiguna dan pertahanan. Perang di Ukraina tidak hanya memicu peningkatan signifikan dalam pengeluaran militer global, tetapi juga menunjukkan kegunaan inovasi teknologi komersial yang siap pakai di medan perang modern. Meskipun platform besar dan sistem senjata tradisional tidak akan kehilangan kepentingannya dalam perang, Ukraina telah merevolusi penggunaan drone murah dan sekali pakai secara ekstensif dan inovatif, yang dimungkinkan oleh sistem dwiguna, seperti Starlink.¹⁵²

Dalam konteks Indonesia modernisasi persenjataan dan penguatan industri pertahanan telah lama menjadi prioritas pemerintah Indonesia, khususnya pemerintah saat ini yang dipimpin oleh Presiden Prabowo Subianto. Pencapaian ambisi modernisasi persenjataan dapat ditelisik dari kecenderungan lonjakan pengeluaran militer

¹⁴⁹ Katja Bego, "How a Surge in Defence and Dual-Use Technology Investment Could Reconfigure the Global AI Race," *Chatham House*, 28 April 2026, <https://www.chathamhouse.org/2026/04/how-surge-defence-and-dual-use-technology-investment-could-reconfigure-global-ai-race/02>.

¹⁵⁰ Corporate Watch, "What's Driving the Militarisation of Tech—and What We Can Do about It," <https://corporatewatch.org/whats-driving-the-militarisation-of-tech-and-what-we-can-do-about-it/>.

¹⁵¹ James W. Hinton, *Dual-Use Technologies in the Age of Intangibles*, Policy Brief No. 215 (Waterloo, ON: Centre for International Governance Innovation [CIGI], 3 November 2025), <https://www.cigionline.org/publications/dual-use-technologies-in-the-age-of-intangibles/>.

¹⁵² Bego, "How a Surge in Defence and Dual-Use Technology Investment."

pada 2025.¹⁵³ Selanjutnya, kenaikan anggaran terlihat pada Rancangan Anggaran Pendapatan dan Belanja Negara (RAPBN) 2027 untuk fungsi Pertahanan, pemerintah menyiapkan anggaran sebesar Rp 329,5 triliun. Angka tersebut naik sekitar Rp 30 triliun, apabila dibandingkan dengan outlook pada Tahun Anggaran 2026, fungsi Pertahanan diperkirakan Rp 299,1 triliun.¹⁵⁴

Kenaikan anggaran secara signifikan menandai kembalinya militerisasi di bawah kepemimpinan Presiden Prabowo Subianto. Menurut Norman Joshua militerisasi di bawah Presiden Prabowo Subianto akan terlihat dalam dua cara (1) peningkatan anggaran militer dan; (2) peran militer yang lebih luas dalam urusan non-keamanan. Peningkatan peran militer dan kepolisian, baik yang masih aktif maupun yang sudah pensiun dalam urusan non-militer kecenderungannya sudah dimulai selama pemerintahan Presiden Joko Widodo. Pada saat bersamaan di bawah kepresidenan Prabowo Subianto terlihat upaya secara sistematis untuk mengembalikan dwifungsi militer yang mencakup tugas pertahanan-keamanan serta tugas sosial-politik.¹⁵⁵ Situasi tersebut oleh Drew Holland Kinney disebut sebagai praetorianisme, yaitu situasi di mana militer memainkan peran dominan dalam struktur dan institusi politik, cenderung sering campur tangan untuk memengaruhi politik dan perubahan konstitusional dan dapat mendominasi sistem politik atau sebaliknya.¹⁵⁶ Anthony Forster mengingatkan bahwa kajian hubungan sipil-militer tidak cukup hanya membahas ancaman intervensi militer dalam politik domestik. Kajian tersebut juga perlu memperhatikan peran aktor-aktor di luar angkatan bersenjata konvensional, seperti kelompok paramiliter dan badan intelijen, yang disebut sebagai kekuatan abu-abu (gray forces).¹⁵⁷

¹⁵³ Meskipun alokasi anggaran 2025 meningkat dibandingkan tahun sebelumnya keraguan masih menyelimuti upaya percepatan modernisasi persenjataan seiring dengan perluasan seiring perluasan organisasi militer Indonesia (TNI) dan anggaran pertahanan yang masih berada di bawah 1% dari PDB. Lihat, Adhi Priamarizki dan Edna Caroline, *Prabowo's Defence Challenge: Making "Triple Helix" Work*, IDSS Paper IP26067 (Singapore: S. Rajaratnam School of International Studies, Nanyang Technological University, 21 Mei 2026), <https://rsis.edu.sg/rsis-publication/idss/ip26067-prabowos-defence-challenge-making-triple-helix-work/>. Outlook fungsi pertahanan sampai akhir 2025 diperkirakan sebesar Rp245,2 triliun atau 147,7% dari pagu APBN 2025. Lihat, Dovana Hasiana, "Anggaran Pertahanan 2025 Dipatok Naik 47% Jadi Rp245 Triliun," *Bloomberg Technoz*, 6 Juli 2025, <https://www.bloombergtechnoz.com/detail-news/76302/anggaran-pertahanan-2025-dipatok-naik-47-jadi-rp245-triliun>.

¹⁵⁴ CNN Indonesia, "Pemerintah Siapkan Rp329,5 Triliun untuk Pertahanan di RAPBN 2027," 19 Agustus 2026, <https://www.cnnindonesia.com/nasional/20260819113956-20-1393907/pemerintah-siapkan-rp3295-triliun-untuk-pertahanan-di-rapbn-2027>.

¹⁵⁵ Michael Breger, "The Legacies of Militarization: Norman Joshua Writes a Social and Cultural History of Indonesian Authoritarianism," FSI, Stanford University, 17 April 2024, <https://fsi.stanford.edu/news/legacies-militarization-norman-joshua-writes-social-cultural-history-indonesian>.

¹⁵⁶ Valerij Shpak, "Indirect Praetorianism: The Case of Turkey's Military," *Scientific Journal of the Military University of Land Forces* 54, no. 4(206) (2022): 624–638, <https://doi.org/10.5604/01.3001.0016.0757>.

¹⁵⁷ Francesco F. Milan, *Three Generations of Studies in Civil-Military Relations: A Primer*, *Revista Científica General José María Córdova*, vol. 24, no. 53, 2026

Perluasan kewenangan TNI yang menjangkau ranah siber yang dinormakan melalui kerangka operasi militer selain perang melalui Undang-Undang Nomor 3 Tahun 2025 justru menegaskan karakteristik ranah siber itu sendiri. Ruang siber memperkenalkan mode koordinasi terdesentralisasi, mengkonfigurasi ulang otoritas, kedaulatan dan tata kelola dan menantang norma kontrol sipil.¹⁵⁸ Militerisme di media sosial mendapatkan legalisasi undang-undang tersebut. Berdasarkan ketentuan Pasal 7 ayat 2 huruf b poin 15 TNI diberikan kewenangan secara atributif untuk membantu upaya menanggulangi ancaman siber. Perluasan peran TNI dalam menanggulangi ancaman siber bisa membuka ruang bagi negara untuk menargetkan pihak-pihak yang hendak memberikan kritik kepada pemerintah. Dampak lebih jauh, kewenangan tersebut dapat mengancam kebebasan berekspresi warga di media sosial.¹⁵⁹

Perluasan kewenangan tersebut kemudian diperkuat melalui Peraturan Presiden (Perpres) Nomor 85 Tahun 2025 merevisi Perpres Nomor 151 Tahun 2024 tentang Kementerian Pertahanan. Berdasarkan regulasi ini Kementerian Pertahanan RI menetapkan nomenklatur baru yakni Badan Informasi dan Komunikasi Intelijen Pertahanan yang memiliki kewenangan m a pengelolaan informasi dan komunikasi intelijen pertahanan.¹⁶⁰ Pembaruan ini kewenangan ini akan menambah kelembagaan yang akan cenderung memperkuat surveilans negara di ruang digital justru berpotensi menciptakan risiko serius bagi kebebasan sipil dan hak-hak fundamental warga negara. Pada titik yang lain Karakteristik ruang siber tersebut semestinya mengubah organisasi dan budaya TNI, termasuk strategi beradaptasi untuk mengkonfigurasi ulang dinamika hubungan sipil-militer dalam ranah siber.

Kewenangan militer juga berpotensi meluas setelah periode stagnasi yang panjang dalam penelitian dan pengembangan antariksa di Indonesia. Sejak menjabat pada Oktober 2024, Presiden Prabowo Subianto berulang kali menekankan pentingnya pengembangan sektor antariksa dalam pidato-pidatonya. Kemudian Pada Januari 2025, Sekretaris Jenderal Asosiasi Antariksa Indonesia, Aryo PS Djojohadikusumo, menyampaikan bahwa Indonesia akan berpartisipasi dalam penelitian antariksa global, dengan Badan Riset dan Inovasi Nasional (BRIN) sebagai lembaga utama yang mengoordinasikan kerja sama dengan berbagai universitas. Selain itu, Indonesia juga berencana meningkatkan infrastruktur antariksa yang sudah usang.

¹⁵⁸ Isabella Neumann, "It Is Complicated: Cyber into the Civil–Military Relationship," *Journal of Cybersecurity* 12, no. 1 (2026): 1–12, <https://doi.org/10.1093/cybsec/tyag012>.

¹⁵⁹ Dewa Ayu Diah Angendari, "Militerisme di Media Sosial: Bagaimana UU TNI Mengancam Kebebasan Sipil di Dunia Siber," *The Conversation*, <https://theconversation.com/militerisme-di-media-sosial-bagaimana-uu-tni-mengancam-kebebasan-sipil-di-dunia-siber-254065>.

¹⁶⁰ Kompas.com, "Kemenhan Bentuk Badan Baru, Diminta Pastikan Tidak Ada Tumpang Tindih," 8 Agustus 2025, <https://nasional.kompas.com/read/2025/08/08/20124741/kemenhan-bentuk-badan-baru-diminta-pastikan-tidak-ada-tumpang-tindih>.

Erna Sri Adiningsih, direktur Badan Antariksa Indonesia (Indonesia Space Agency/INASA) yang dibentuk di bawah BRIN,¹⁶¹ mengatakan rencana antariksa Indonesia berfokus pada peningkatan teknologi antariksa, analisis dan pengolahan data jarak jauh, serta keamanan antariksa melalui kerja sama internasional.¹⁶² Pada 24 Juni 2025, Universitas Pertahanan Republik Indonesia (Unhan RI) meluncurkan satelit nano RIDU-Sat 1. Peluncuran menggunakan roket Falcon 9 Transporter 14 Rideshare milik SpaceX.¹⁶³ Komitmen untuk memanfaatkan luar angkasa semakin menguat Ketika Komando Operasi Udara Nasional Indonesia secara resmi membentuk Unit Antariksa khusus pada Januari 2026. Kepala Staf Angkatan Udara sebelumnya menyatakan secara terbuka bahwa masa depan pertahanan Indonesia terletak di luar angkasa, dan kendali atas domain ini akan menjadi kunci kedaulatan nasional di era modern. Namun demikian, Unit Antariksa tersebut masih kekurangan landasan hukum yang jelas untuk mendukung kewajiban domestik dan internasional Indonesia yang terikat dengan perjanjian tentang hukum angkasa.¹⁶⁴

Sementara itu, berdasarkan data Indonesia National Procurement Portal (Inaproc), tercantum paket penyedia 63689327 berupa sistem monitoring sosial media dengan pagu anggaran Rp 49.235.461.000. Paket pengadaan sistem monitoring media sosial senilai Rp 49,2 miliar oleh Kementerian Pertahanan tahun anggaran 2026 Metode pemilihan penyedia barang dan jasa adalah melalui penunjukan langsung dengan satuan kerja (satker) Mabes TNI Angkatan Darat. Jadwal pelaksanaan kontrak dimulai pada Februari 2026 dan berakhir pada Februari 2026.¹⁶⁵ Meskipun kemudian, TNI Angkatan Darat menyatakan, kontrak pengadaan *monitoring* media sosial belum dilakukan dengan pihak mana pun, termasuk untuk paket pengadaan sistem *monitoring* media sosial senilai Rp49,2 miliar.¹⁶⁶

¹⁶¹ Sebagai bagian dari mandatnya, BRIN menyediakan bantuan teknologi penginderaan jauh berbasis satelit kepada pemerintah, memberikan peran sentral kepada pemerintah dalam aplikasi terkait ruang angkasa untuk pembangunan ekonomi, penegakan hukum, dan pertahanan nasional. Lihat, University World News, "Indonesia Ramps Up Space R&D to Reduce Foreign Reliance," 25 November 2025, <https://www.universityworldnews.com/post.php?story=20251125121827251>.

¹⁶² University World News, "Indonesia Ramps Up Space R&D."

¹⁶³ Kementerian Pertahanan Republik Indonesia, "Unhan RI Sukses Luncurkan Satelit Nano Indonesia, RIDU-Sat 1," 25 Juni 2025, <https://www.kemhan.go.id/2025/06/25/unhan-ri-sukses-luncurkan-satelit-nano-indonesia-ridu-sat-1.html>.

¹⁶⁴ Taufik Rachmat Nugraha dan Bich Tran, *Bridging the Legal and Strategic Mismatch in the Indonesian Air Force's Space Unit*, IDSS Paper IP26100 (Singapore: S. Rajaratnam School of International Studies, Nanyang Technological University, 27 Agustus 2026), <https://rsis.edu.sg/rsis-publication/idss/ip26100-bridging-the-legal-and-strategic-mismatch-in-the-indonesian-air-forces-space-unit/>.

¹⁶⁵ Kompas.id, "Publik Pertanyakan Anggaran Rp 49,2 Miliar untuk Monitoring Medsos TNI AD," 29 April 2026, <https://www.kompas.id/artikel/anggaran-rp-492-miliar-untuk-monitoring-medsos-tni-ad-dipertanyakan-publik>.

¹⁶⁶ Kompas.id, "Kadispenad: Kontrak Monitoring Medsos Rp 49,2 Miliar Tidak Pernah Dilaksanakan," 30 April 2026, <https://www.kompas.id/artikel/kadispenad-kontrak-monitoring-medsos-rp-492-miliar-tidak-pernah-dilaksanakan>.

Pada saat bersamaan sampai saat ini, Indonesia juga tidak memiliki undang-undang yang secara khusus mengatur penggunaan *spyware* dan teknologi pengawasan secara sah. Situasi ini diperburuk karena budaya politik Indonesia membuat ekosistem piranti *spyware* semakin mengkhawatirkan sehingga semakin sulit untuk mendeteksi kasus penyalahgunaan ilegal terhadap masyarakat sipil. Konsekuensi lebih jauh, situasi ini berisiko menciptakan impunitas yang dirancang untuk pelanggaran HAM.¹⁶⁷ Pada titik yang lain langkah-langkah pengendalian ekspor Indonesia paling tidak selaras dengan norma global. Indonesia bukan anggota rezim pengendalian ekspor multilateral mana pun, dan juga tidak memiliki daftar barang-barang dwiguna untuk dikendalikan. Penolakan Jakarta terhadap pengendalian perdagangan strategis muncul dari kekhawatiran pengendalian barang dwiguna yang dikembangkan oleh negara-negara maju bersifat diskriminatif terhadap negara-negara berkembang dan dapat menghambat akses Indonesia terhadap teknologi dwiguna.¹⁶⁸ Sering kali *spyware* telah dianggap sebagai alat penting untuk penegakan hukum dan operasi intelijen. Namun, banyak contoh negara yang menggunakannya dengan cara yang melanggar HAM merusak demokrasi dan supremasi hukum.¹⁶⁹

Laporan Amnesty International dengan judul *Membangun Musuh Khayalan* memperlihatkan manifestasi kewenangan TNI untuk menangani operasi militer selain perang. Laporan Amnesty Internasional menyebutkan adanya dugaan keterlibatan otoritas Indonesia, termasuk militer menggunakan disinformasi online untuk menargetkan jurnalis, aktivis, akademisi, dan demonstran sebagai pembalasan atas aktivisme dan ekspresi sah mereka.¹⁷⁰ Kasus Andrie Yunus, wakil koordinator Komisi untuk Orang Hilang dan Korban Kekerasan (KontraS) memperlihatkan adanya pola keterkaitan antara kampanye online yang terkoordinasi dan serangan fisik tersebut. Andrie Yunus telah menjadi target kampanye online terkoordinasi yang menggambarkannya sebagai "agen asing" setelah beberapa kali melakukan protes damai terhadap revisi UU TNI selama berbulan-bulan.¹⁷¹

¹⁶⁷ Amnesty International, *A Web of Surveillance*.

¹⁶⁸ Matthew P. Goodman, Matthew Reynolds, dan Julianne Fittipaldi, *Economic Security in Emerging Markets: A Look at India, Vietnam, and Indonesia*, CSIS Brief (Washington, DC: Center for Strategic and International Studies (CSIS), 17 Mei 2022), <https://www.csis.org/analysis/economic-security-emerging-markets-look-india-vietnam-and-indonesia>.

¹⁶⁹ Lena Riecke, "Unmasking the Term 'Dual Use' in EU Spyware Export Control," *European Journal of International Law* 34, no. 3 (2023): 697–720, <https://doi.org/10.1093/ejil/chad039>.

¹⁷⁰ Amnesty International, "Indonesia: Military Silences Dissent with Disinformation Campaigns Branding Activists and Journalists 'Foreign Agents'," 19 Mei 2026, <https://www.amnesty.org/en/latest/news/2026/05/indonesia-military-silences-dissent-disinformation-campaigns-branding-activists-journalists-foreign-agents/>.

¹⁷¹ Amnesty International, *Membangun Musuh Khayalan: Misinformasi, Disinformasi dan Tuduhan "Antek Asing" di Bawah Presiden Prabowo di Indonesia*, ASA 21/0931/2026 (19 Mei 2026), <https://www.amnesty.org/en/documents/asa21/0931/2026/id/>.

Insiden ini tidak terjadi semerta-merta; insiden itu telah lama direncanakan dan telah didahului oleh kampanye serangan disinformasi daring yang terorganisir serta melibatkan beberapa aktor - yang dirancang untuk merusak kredibilitas dan mendelegitimasi karirnya sebagai pembela HAM menggunakan label “antek asing” – dan upaya luring berkelanjutan untuk mengintimidasi dirinya

Komisaris Tinggi PBB untuk Hak Asasi Manusia, Michelle Bachelet menyatakan.¹⁷²

Kekhawatiran serius tentang bahaya penggunaan alat pengawasan oleh pihak berwenang dari berbagai sumber yang seharusnya meningkatkan keamanan publik untuk meretas telepon dan komputer orang-orang yang melakukan kegiatan jurnalistik yang sah, memantau hak asasi manusia, atau mengekspresikan perbedaan pendapat atau oposisi politik.

Pemerintah harus segera menghentikan penggunaan teknologi pengawasan mereka sendiri dengan cara yang melanggar hak asasi manusia, dan harus mengambil tindakan konkret untuk melindungi dari pelanggaran privasi tersebut dengan mengatur distribusi, penggunaan, dan ekspor teknologi pengawasan yang dibuat oleh pihak lain.

Pandangan senada juga disampaikan Gina Romero, Pelapor Khusus tentang Pelapor Khusus tentang kebebasan berkumpul secara damai dan berorganisasi (Special Rapporteur on freedom of peaceful assembly and of association) menyatakan.¹⁷³

Narasi narasi tentang agen asing sering dilabelkan dan ditujukan kepada masyarakat sipil dan para pengunjuk rasa. Pelabelan ini seringkali mendasarkan tuduhan tersebut pada jenis pendanaan yang mereka terima. Masyarakat sipil yang menerima pendanaan asing secara eksplisit diincar dan diserang dengan pelecehan dan kampanye stigmatisasi. Pelabelan ini disertai dengan surveilans yang berlebihan dan potensi pembatasan akses terhadap sumber daya bagi masyarakat sipil. Stigmatisasi agen asing semakin melemahkan kepercayaan publik yang dibutuhkan agar masyarakat sipil dapat melakukan pekerjaannya.

Narasi-narasi ini telah menjadi instrumen yang meluas untuk stigmatisasi dengan tujuan mendelegitimasi para aktivis dan asosiasi, dan didukung serta diperkuat oleh adopsi luas dari apa yang disebut hukum “agen asing”. Narasi ini mengakibatkan

¹⁷² Office of the United Nations High Commissioner for Human Rights (OHCHR), “Use of Spyware to Surveil Journalists and Human Rights Defenders: Statement by UN High Commissioner for Human Rights Michelle Bachelet,” 19 Juli 2021, OHCHR.

¹⁷³ Gina Romero, *Protecting the Rights to Freedom of Peaceful Assembly and of Association from Stigmatization*, Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, UN Doc. A/79/263 (United Nations, 31 Juli 2024), https://digitallibrary.un.org/record/4059940/files/A_79_263-EN.pdf.

kriminalisasi dan, di beberapa negara, pembubaran massal organisasi masyarakat sipil yang ditetapkan sebagai agen asing.

Hal ini semakin didukung oleh kampanye fitnah terhadap organisasi masyarakat sipil yang menerima dana dari luar negeri, termasuk publikasi oleh pihak berwenang atas daftar organisasi tersebut. Daftar tersebut juga telah dipublikasikan di media sosial atau oleh media massa yang menggunakan bahasa stigmatisasi negatif, yang menargetkan baik organisasi pemberi dana maupun organisasi masyarakat sipil itu sendiri, serta staf mereka, memperkuat stigmatisasi dan mengekspos mereka pada ujaran kebencian, pencemaran nama baik, dan serangan.

6. Teknologi Dwiguna dalam Konteks Kompleks Digital Industrial Militer: Demarkasi Sipil dan Militer yang Semakin Kabur

Perkembangan pesat persenjataan konvensional canggih dan teknologi militer sejak tahun 1990-an terjadi pada periode ketika teknologi yang relevan secara militer (*militarily relevant technologies*) semakin sulit untuk diidentifikasi dan diklasifikasikan. Banyak teknologi komersial canggih menawarkan peluang baru dan berpotensi signifikan untuk aplikasi pertahanan sehingga dapat memengaruhi kekuatan militer dan metrik keunggulan militer. Bahkan sebelum berakhirnya Perang Dingin, teknologi dan inovasi teknologi yang dirancang dan dikembangkan di sektor teknologi tinggi komersial jelas lebih unggul dan lebih murah daripada yang ditemukan di kompleks industri militer.¹⁷⁴ Keunggulan teknologi komersial ini menjadi semakin jelas dalam beberapa tahun terakhir mengingat munculnya revolusi industri keempat yang berputar di sekitar teknologi-teknologi baru, seperti kecerdasan artifisial, sistem otonom, big data, dan komputasi kuantum. Pada saat yang sama, teknologi-teknologi ini dan produk-produk terkaitnya membuat perbedaan antara teknologi militer dan sipil dan, secara lebih luas, perbedaan antara inovasi berbasis militer dan sipil – semakin sulit untuk dibedakan.¹⁷⁵ Seiring perkembangan tersebut, batas antara sektor sipil dan militer semakin luruh, khususnya di bidang antariksa, siber, dan kecerdasan artifisial. Demarkasi sipil dan

¹⁷⁴ Yoram Evron dan Richard A. Bitzinger, *The Fourth Industrial Revolution and Military-Civil Fusion: A New Paradigm for Military Innovation?* (Cambridge: Cambridge University Press, 2023).

¹⁷⁵ Secara khusus, tahap-tahap akhir dari apa yang disebut revolusi industri ketiga (third industrial revolution) yang berpusat pada terobosan dalam mikroelektronika, komputasi, telekomunikasi, dan teknologi informasi lainnya – sebagian besar didominasi oleh inovasi yang berpusat di bidang komersial, misalnya, di tempat-tempat seperti Silicon Valley atau inkubator teknologi Israel, atau di perusahaan-perusahaan seperti Google, Amazon, dan Alibaba. Lihat, Evron dan Bitzinger, *The Fourth Industrial Revolution and Military-Civil Fusion*.

militer yang semakin kabur ini mendorong era baru kolaborasi sipil-militer yang siap mengubah wajah keamanan nasional dan inovasi teknologi.¹⁷⁶

Seiring dengan perkembangan tersebut, kekhawatiran teknologi dwiguna muncul bersamaan dengan ketakutan berkembangnya proliferasi teknologi terkait senjata nuklir pada awal Perang Dingin. Kekhawatiran ini mengarah pada target yang jelas, seperti baja khusus, piranti dan fasilitas manufaktur berbantuan komputer presisi tinggi, dan piranti lunak dan piranti keras berkinerja tinggi; meliputi material dan piranti yang mudah diadaptasi untuk desain dan manufaktur terkait senjata nuklir. Baru-baru ini, fokus telah bergeser ke konteks teknologi non-nuklir, termasuk, teknologi biologi dan informasi yang terus dilakukan penelitian dan pengembangan yang berkelanjutan yang secara dramatis meningkatkan kesejahteraan sosial dan ekonomi manusia, meskipun dengan mengorbankan potensi teknologi ini untuk dimanfaatkan untuk tujuan jahat.¹⁷⁷

Istilah dwiguna (*dual-use*) awalnya merujuk pada serangkaian material nuklir tertentu setelah Perang Dunia II yang dapat digunakan untuk tujuan militer (senjata) dan sipil (energi). Saat ini, istilah dwiguna diterapkan lebih luas untuk mencakup perusahaan yang produknya dapat memenuhi kebutuhan pemerintah. Export Administration Regulations mendefinisikan barang dwiguna sebagai barang yang memiliki aplikasi sipil dan potensi penggunaan dalam terorisme, militer, atau senjata pemusnah massal (*weapons of mass destruction*). Dalam konteks investasi, seperti European Investment Fund, investasi dwiguna kini diterima selama tidak termasuk senjata dan amunisi. Namun, membedakan antara teknologi untuk penggunaan sipil dan militer menjadi semakin menantang karena garis antara solusi ofensif dan defensif semakin kabur. Implikasi lebih jauh, bagi sebagian investor, memutuskan di mana harus menarik garis antara mendukung teknologi untuk perang atau perdamaian tetap menjadi isu yang kompleks dan diperdebatkan.¹⁷⁸

Jake Chapman memaknai teknologi dwiguna dengan mempertimbangkan empat kategori yang lebih spesifik, meliputi: ¹⁷⁹

1) Komersial/Komersial (*Commercial/Commercial*):

Penggunaan teknologi ini, termasuk teknologi yang dikembangkan untuk pasar komersial dan sebagian besar tetap bersifat komersial. Penggunaan teknologi ini disebut teknologi komersial siap pakai (*commercial off-the-shelf*). Teknologi ini

¹⁷⁶ Gonçalo Lopes, "From Orbit to Cyber Wars: The New Era of Civil-Military Synergy," *VisionSpace*, 25 Maret 2025, <https://visionspace.com/from-orbit-to-cyber-wars-the-new-era-of-civil-military-synergy/>.

¹⁷⁷ Robert Rosner, "Preface," dalam *Governance of Dual-Use Technologies: Theory and Practice*, disunting oleh Elisa D. Harris (Cambridge, MA: American Academy of Arts and Sciences, 2016).

¹⁷⁸ "Defining 'Dual-Use'," *Defining 'Dual-Use' | Dual-Use Readiness Model* (<https://dualuse.mit.edu/defining-dual-use/>), diakses pada 19 Agustus 2026

¹⁷⁹ Jake Chapman, *Reliance on Dual-Use Technology Is a Trap*, *Reliance on Dual-Use Technology Is a Trap* (<https://warontherocks.com/reliance-on-dual-use-technology-is-a-trap/>), diakses pada 28 Agustus 2026

dapat berbentuk piranti keras atau peranti lunak yang sudah ada di pasar komersial dan tersedia untuk dijual kepada publik. Teknologi siap pakai karena dirancang sesuai dengan standar industri yang ketat dan dengan investasi swasta yang substansial. Penggunaan teknologi ini semuanya mengarah pada solusi yang terus disempurnakan dan dapat diadopsi dengan biaya rendah serta dibuat dalam skala besar;

2) Pertahanan/Komersial (*Defense/Commercial*)

Teknologi ini berasal dari bidang pertahanan tetapi memiliki pasar komersial masa depan yang substansial. Kategori ini mencakup banyak teknologi dwiguna yang menjadi fondasi Silicon Valley, tetapi kini semakin berkurang dalam ekosistem teknologi setiap tahunnya. Teknologi yang sedang dikembangkan saat ini dapat dikatakan termasuk dalam kategori Pertahanan/Komersial, meliputi penerbangan hipersonik dan metode canggih untuk penentuan posisi, navigasi, dan waktu, seperti piranti canggih untuk Sistem Penentuan Posisi Global (GPS). Kategori ini bukanlah teknologi yang paling banyak dicari pendanaannya oleh para investor modal ventura, dan bukan pula yang dibicarakan oleh sebagian besar orang dalam inovasi pertahanan di bawah payung dwiguna;

3) Pertahanan/Pertahanan (*Defense/Defense*)

Kontraktor utama, pada gilirannya, secara konvensional berfokus pada teknologi yang berasal dari bidang pertahanan dan sebagian besar akan tetap berfokus pada pasar pertahanan. Kategori ini mencakup amunisi inovatif, semua platform canggih seperti pesawat tempur, pesawat pengebom, dan kapal, serta aplikasi yang sangat khusus dari teknologi tertentu, seperti kecerdasan artifisial. Kategori ini hanya merupakan teknologi dwiguna dalam definisi yang paling liberal dan cenderung menerima pendanaan modal ventura swasta paling sedikit;

4) Komersial/Pertahanan (*Commercial/Defense*)

Meskipun semua kategori di atas menggambarkan kemampuan yang secara teknis bersifat ganda, kategori teknologi ini mengutamakan komersial terlebih dahulu dan kemudian untuk kepentingan pertahanan. Kategori ini mendapatkan perhatian dari komunitas modal ventura dan komunitas pertahanan, khususnya di Amerika Serikat. Kategori teknologi ini rentan terhadap peretasan. Departemen Pertahanan Amerika Serikat semakin mempromosikan teknologi dwiguna kategori komersial/pertahanan melalui perusahaan rintisan. Perusahaan rintisan akan didorong untuk mengembangkan produk komersial terlebih dahulu dan berhasil mengembangkan bisnis di pasar komersial. Setelah perusahaan rintisan mencapai kesuksesan komersial yang cukup untuk bertahan dalam labirin akuisisi pertahanan

yang rumit, barulah perusahaan rintisan ini mencoba mengadaptasi produk mereka untuk militer.

Sementara menurut Gene Keselman dan Fiona Murray teknologi dwiguna merupakan strategi pasar yang mungkin diterapkan dengan mengutamakan pertahanan, komersial, atau keduanya. Saat ini, istilah tersebut digunakan secara longgar untuk mencakup berbagai macam perusahaan yang produk dan layanannya dapat memecahkan masalah militer maupun sipil. Dalam konteks investasi, pendana besar seperti Dana Investasi Eropa (European Investment Fund) telah mengecualikan usaha yang membangun solusi penggunaan ganda untuk pertahanan. Sementara yang lain hanya menganggap usaha-usaha ini layak didukung, jika pasar komersial dieksplorasi terlebih dahulu atau merupakan mayoritas penjualan. Dalam perkembangannya setiap kondisi batas ini semakin luruh. Menurut European Investment Fund, investasi yang disebut sebagai investasi dwiguna kini batasannya hanya ditarik untuk mengecualikan amunisi dan senjata. Pada saat yang sama sebagai kategori teknologi dwiguna terus membingungkan investor dan pasar karena kurangnya definisi yang jelas dan bermanfaat untuk membangun koridor yang jelas dan terukur.¹⁸⁰

Pada titik yang lain, bagi investor, teknologi dwiguna harus dipahami sebagai strategi yang akan membentuk rencana dan prioritas serta menekankan adopsi etis dalam semua kasus penggunaan teknologi tersebut. Strategi dwiguna, terlepas dari apakah itu mengutamakan pertahanan atau berjalan paralel dengan kasus penggunaan sipil, seperti strategi masuk pasar lainnya berkaitan dengan kompromi: solusi mana yang akan dibangun dan untuk siapa, bagaimana mengujinya, bagaimana mendanainya, dan bagaimana menerapkannya dengan tepat. Selanjutnya Gene Keselman dan Fiona Murray, mengidentifikasi tiga dimensi untuk menelisik teknologi dwiguna, mencakup: (1) dimensi pelanggan; (2) dimensi pendanaan; dan (3) dimensi teknologi.¹⁸¹ Urain ketiga dimensi teknologi dwiguna dapat dilihat melalui tabel di bawah ini.¹⁸²

Dimensi Teknologi Dwiguna	Deskripsi
Pelanggan	Pasar komersial dan pertahanan sangat berbeda. Pasar komersial biasanya memiliki persaingan yang ketat, fokus pada inovasi yang cepat, dan hubungan langsung antara pelanggan dan produk. Produsen memiliki pelanggan yang menuntut dan berfokus pada efisiensi ekonomi. Sebaliknya, pasar misi sering beroperasi dalam lingkungan yang lebih terstruktur, dengan jangka

¹⁸⁰ Gene Keselman dan Fiona Murray, "Dual-Use Is a Strategy, Not a Category (Nor a Trap)," *War on the Rocks*, 2 Januari 2025, <https://warontherocks.com/dual-use-is-a-strategy-not-a-category-nor-a-trap/>.

¹⁸¹ Keselman dan Murray, "Dual-Use Is a Strategy, Not a Category."

¹⁸² Keselman dan Murray, "Dual-Use Is a Strategy, Not a Category."

	waktu yang panjang, peraturan yang ketat, dan jaringan pemangku kepentingan yang kompleks. Pelanggan pemerintah beroperasi di bawah serangkaian peraturan yang kompleks dan dengan kosakata khusus.
Pendanaan	Usaha komersial sering kali bergantung pada modal yang disebut sebagai dilutif, yaitu pendanaan dari investor individu atau venture capitalist (investor institusional) dengan cara mengambil saham ekuitas dalam usaha tersebut. Pendanaan pemerintah, yang disebut non-dilutif dan dapat berbentuk hibah dan kontrak dari kantor pemerintah tertentu. Meskipun pendanaan ini biasanya tidak mengharuskan pelepasan ekuitas atau kepemilikan dan kompleksitas kontraktual. Pendanaan pemerintah dapat memberikan peluang untuk mendukung beberapa penelitian dan pengembangan, kemudian pada tahap selanjutnya biasanya terdapat pendanaan yang lebih besar, Namun demikian, hal ini melibatkan labirin peraturan dan persyaratan kepatuhan, termasuk ruang lingkup pekerjaan dan hasil yang diharapkan
Teknologi	Meskipun solusi dasarnya mungkin serupa untuk konteks komersial dan pertahanan, cara kemajuan teknologi dijelaskan dan diukur dapat berbeda secara signifikan. Dalam konteks pertahanan dan pemerintahan yang lebih luas, teknologi harus memenuhi spesifikasi, persyaratan, dan kepatuhan yang ketat terhadap standar, seperti spesifikasi militer dan tingkat kesiapan teknologi. Meskipun tujuannya adalah untuk memperoleh kemampuan yang memenuhi kebutuhan misi, persyaratan teknologi yang tepat ini dirancang untuk memastikan kompatibilitas dan efektivitas dalam sistem misi yang lebih luas. Pengguna misi mengharapkan bukti kemajuan melalui proses formal seperti uji coba lapangan, uji operasional dan evaluasi, dan simulasi seperti permainan perang yang mereplikasi skenario dunia nyata.

Logika dwiguna bukanlah hal baru, militer selalu menargetkan warga sipil dan ruang sipil untuk memperoleh keuntungan atas musuh yang berperang.¹⁸³ Dengan preseden penting sejarah perang, maka dari konteks ini dirumuskan dan direvisi serangkaian infrastruktur hukum kemanusiaan yang didasarkan pada perbedaan antara warga sipil dan kombatan, serta mekanisme tata kelola internasional seperti hukum pidana internasional, Mahkamah Internasional (*International Court of Justice*), Mahkamah Pidana Internasional (*International Criminal Court*), dan hukum humaniter internasional. Konvensi Jenewa 1949 dan Protokol Tambahan Konvensi Jenewa 1977 yang mengatur hukum humaniter dirancang justru untuk mencegah runtuhnya kategori sipil dan militer. Ketidadaan pembeda antara kategori sipil dan militer yang menjadi dasar kehancuran Perang Dunia Kedua dan kekerasan perang-perang berikutnya pada tahun 1950-an dan 1960-an. Prinsip pembedaan¹⁸⁴ menegaskan para peserta dalam suatu konflik 'harus setiap saat membedakan antara penduduk sipil dan kombatan serta antara objek sipil dan sasaran militer dan karenanya harus mengarahkan operasi mereka hanya terhadap sasaran militer.'¹⁸⁵ Teknologi-teknologi ini semakin menjadi pusat keamanan nasional, ketahanan ekonomi, dan kepemimpinan teknologi. Teknologi dwiguna menjadi semakin penting bagi pertumbuhan ekonomi suatu negara dan kemampuan negara tersebut untuk mempertahankan diri. Teknologi ini sangat penting untuk mendorong daya saing, ketahanan, dan pertahanan serta keamanan nasional yang krusial, terutama dalam lingkungan geopolitik internasional yang penuh ancaman saat ini.¹⁸⁶

Di antara bidang-bidang yang telah mengikis perbedaan antara produksi peralatan militer dan keamanan¹⁸⁷ dan meningkatnya pentingnya teknologi sipil dan barang-barang dwiguna (*dual-use items*) di bidang ini. Negara-negara dan produsen senjata memperluas jangkauan situasi penggunaan teknologi sipil dalam produksi peralatan militer dan keamanan. Akibatnya, teknologi dan sistem yang sebelumnya diklasifikasikan sebagai sipil mungkin perlu diklasifikasikan ulang sebagai barang dwiguna, yaitu, barang,

¹⁸³ Dalam sejarah militer, penggunaan ganda merupakan andalan peperangan, misalnya, angkatan udara Sekutu dan Jerman sama-sama membombardir kota-kota Eropa selama Perang Dunia Kedua, dan Angkatan Udara Amerika Serikat menargetkan desa, kota kecil, dan kota besar selama kampanyenya di Vietnam, Laos, dan Kamboja. Perang-perang tersebut ditandai dengan bentuk kekerasan militer yang tidak membedakan antara ruang sipil dan militer atau, sebaliknya, memanfaatkan perbedaan tersebut sebagai sarana untuk mendemoralisasi musuh. Lihat, Jones, Mousamputri, dan Griffiths, "Dual Use as a Political Technology of Contemporary Military Violence."

¹⁸⁴ Prinsip pembedaan merupakan prinsip hukum terpenting dalam perang yang menjadi dasar bagi semua prinsip lainnya. Sebagai contoh, prinsip proporsionalitas sebagai penyeimbangan antara tujuan dan kebutuhan militer dengan potensi bahaya bagi warga sipil dan objek sipil sepenuhnya bergantung pada identifikasi dan kemudian pendefinisian sifat sipil. Lihat, Jones, Mousamputri, dan Griffiths, "Dual Use as a Political Technology of Contemporary Military Violence."

¹⁸⁵ Jones, Mousamputri, dan Griffiths, "Dual Use as a Political Technology of Contemporary Military Violence."

¹⁸⁶ Hinton, *Dual-Use Technologies in the Age of Intangibles*.

¹⁸⁷ Peralatan militer dan keamanan yaitu, peralatan yang dikembangkan dan digunakan untuk tujuan militer dan keamanan yang dilakukan oleh angkatan bersenjata, lembaga penegak hukum, lembaga intelijen, dan perusahaan keamanan swasta. Lihat Hinton, *Dual-Use Technologies in the Age of Intangibles*.

perangkat lunak, dan teknologi yang dapat digunakan untuk aplikasi sipil dan militer. Negara-negara juga mendorong perusahaan dan lembaga penelitian dan akademis untuk mengembangkan teknologi dan sistem yang diwujudkan berdasarkan desain dan dapat dimasukkan ke dalam piranti militer dan keamanan atau digunakan sebagai peralatan militer dan keamanan. Proses ini dapat menciptakan kategori baru barang diwujudkan.¹⁸⁸

Pergeseran ini menciptakan risiko baru bagi pemerintah, perusahaan, dan lembaga penelitian serta akademis yang terlibat. Perluasan jangkauan situasi penggabungan teknologi sipil ke dalam peralatan militer dan keamanan, serta penciptaan teknologi dan sistem yang memiliki fungsi ganda berdasarkan desain, membentuk jalur baru yang memungkinkan produksi peralatan militer dan keamanan. Hal ini juga meningkatkan jangkauan perusahaan dan lembaga penelitian serta akademis yang secara langsung atau tidak langsung terlibat dalam produksi peralatan militer dan keamanan. Pergeseran ini menciptakan jalan baru yang memungkinkan peralatan militer dan keamanan menjangkau pelaku tindak pidana, teroris, atau negara yang mungkin menggunakannya sehubungan dengan pelanggaran hukum HAM internasional atau hukum humaniter internasional.¹⁸⁹ Pergeseran ini dan risiko yang ditimbulkannya ditunjukkan dalam kasus teknologi pengenalan wajah (*facial recognition technologies*) merupakan jenis teknologi biometrik yang dapat digunakan untuk mengenali identitas seseorang berdasarkan fitur wajah. Teknologi ini sebagian besar telah dikembangkan di sektor sipil dan memiliki berbagai aplikasi sipil, tetapi juga diintegrasikan ke dalam peralatan militer dan keamanan. Kekhawatiran tentang risiko pengalihan dan penyalahgunaan telah muncul sehubungan dengan teknologi pengenalan wajah dan peralatan militer dan keamanan yang menggabungkan teknologi ini.¹⁹⁰

Demikian pula ruang angkasa bukan lagi arena bermain eksklusif pemerintah. Operasi militer kontemporer semakin bergantung pada perusahaan satelit swasta yang menyediakan layanan intelijen dan komunikasi di seluruh dunia. Satelit kini dapat dimanfaatkan untuk mendukung koordinasi medan perang dan operasi militer. Sebuah satelit yang menyediakan akses internet kepada warga sipil, pada saat yang sama, dapat memungkinkan kontrol militer.¹⁹¹ Sejak Perang Dingin, satelit militer telah digunakan

¹⁸⁸ Mark Bromley dan Giovanna Maletta, *The Militarization of Technology: Preventing Diversion and Misuse Through Export Controls*, SIPRI Research Policy Paper (Stockholm: Stockholm International Peace Research Institute (SIPRI), November 2025), <https://doi.org/10.55163/VDOD7802>.

¹⁸⁹ Bromley dan Maletta, *The Militarization of Technology*.

¹⁹⁰ Jenis-jenis teknologi pengenalan wajah dan peralatan militer dan keamanan tertentu yang menggabungkan teknologi pengenalan wajah sudah tercakup dalam kontrol ekspor negara. Uni Eropa (UE) dan Amerika Serikat juga telah membahas pembuatan kategori baru kontrol ekspor untuk menangkap teknologi ini. Lihat, Bromley dan Maletta, *The Militarization of Technology*.

¹⁹¹ Sofia Niiles, "Dual-Use Satellites and the Law of Armed Conflict: The Tension Between Targeting Rules and State Responsibility in Outer Space," *Amsterdam Law Forum*, 10 Juni 2026, <https://vu.nl/en/news/2026/dual-use-satellites-and-the-law-of-armed-conflict>.

untuk menciptakan saluran komunikasi yang aman, untuk manuver dan koordinasi pasukan militer dan penargetan rudal. Namun, ada penggunaan satelit yang berbeda, yang tidak secara langsung terkait dengan operasi militer, yang dipergunakan untuk kepentingan intelijen, surveilans, dan pengintaian (intelligence, surveillance, and reconnaissance). Dalam aktivitas intelijen, surveilans, dan pengintaian, satelit sipil menjadi sumber data dan informasi yang berharga. Satelit meteorologi menyediakan informasi cuaca yang sangat penting untuk pelaksanaan operasi tanpa risiko kerugian yang disebabkan oleh kondisi atmosfer. Satelit ilmiah dan komersial dapat menjual jasanya kepada angkatan bersenjata, sehingga menyediakan data tanpa berada di bawah kendali langsung militer. Dalam semua aplikasi ini, satelit secara tidak langsung menjadi instrumen perang. Namun, satelit tidak digunakan sebagai platform senjata, karena hal itu akan melanggar konsensus internasional saat ini yang menentang militerisasi ruang angkasa. Meskipun ketentuan dalam Perjanjian Luar Angkasa (Space Treaty), 1967 secara jelas melarang penempatan senjata pemusnah massal dan pembangunan instalasi militer, perjanjian tersebut tidak mengatur penggunaan satelit sebagai instrumen perang tidak langsung. Oleh karena itu, setiap upaya untuk mengatur penggunaannya dalam peperangan perlu mempertimbangkan sifat ganda yang melekat pada data satelit.¹⁹²

Intervensi Elon Musk selama invasi Rusia ke Ukraina merupakan salah satu contoh bagaimana teknologi luar angkasa telah mengubah jalannya konflik bersenjata. Elon Musk melalui perusahaannya, Starlink, menyediakan infrastruktur komunikasi dan kemampuan surveilans bagi pasukan Ukraina dan Rusia. Namun, Elon Musk secara konsisten membatasi akses ke layanan tersebut di kedua pihak, yang menggarisbawahi bagaimana satu aktor swasta dapat memengaruhi operasi militer yang dulunya dikelola oleh negara.¹⁹³ Peran dualitas Starlink sebagai infrastruktur teknologi dan sebagai piranti geopolitik menjadi kenyataan pahit di Gaza. Sejak Oktober 2023, pemboman tanpa henti Israel telah menghancurkan sebagian besar jaringan komunikasi di wilayah tersebut, menyebabkan rumah sakit, ambulans, dan lembaga bantuan terputus. Keterlibatan Starlink di Gaza, ketika Israel menargetkan infrastruktur telekomunikasi Gaza, menyebabkan pemadaman listrik bagi 2,3 juta warga Palestina, Starlink dengan cepat diaktifkan untuk Pasukan Pertahanan Israel (IDF). Tentara Israel (IDF) telah membunuh sekitar 60.000 warga Palestina sebagian besar adalah perempuan dan anak-anak. Kemudian pada 27 Oktober, pemadaman komunikasi total Israel di Gaza

¹⁹² Danilo delle Fave, "The Challenges of Dual-Use Space Technologies: The Non-Peaceful Use of Satellites," *Space Generation Advisory Council*, 14 April 2023, <https://spacegeneration.org/the-challenges-of-dual-use-space-technologies-the-non-peaceful-use-of-satellites>.

¹⁹³ Alyssa Macaluso, "Space Is Not a Human Rights Vacuum," *Science & Politics*, 25 Februari 2026, <https://sciencepolitics.org/2026/02/25/space-is-not-a-human-rights-vacuum/>.

mendorong Elon Musk untuk menjanjikan dukungan Starlink bagi organisasi bantuan yang diakui secara internasional.¹⁹⁴

Situasi tersebut memperlihatkan teknologi politik dwiguna (*political technology of dual use*) mengaburkan dunia militer dan non-militer untuk melegitimasi kekerasan militer. Terkadang dan dengan tingkat yang berbeda di wilayah perang, segala sesuatu dapat menjadi sasaran atau dilarang, setiap orang bersalah dan dapat dibunuh; rumah sakit adalah gudang militer, bahan bangunan adalah komponen bom, dan warga sipil adalah kombatan. Hampir semua dimasukkan dalam logika peperangan dan dengan demikian hampir semuanya dapat dihancurkan, mulai dari manusia dan rumah hingga obat-obatan dan makanan yang menopang kehidupan. Teknologi dwiguna telah menjadi teknologi politik penting yang menjadi pusat distribusi kekerasan militer kontemporer.¹⁹⁵

Saat ini negara dan militer telah menggunakan kerangka kerja dwiguna Hukum Humaniter Internasional sehingga memungkinkan operasi di ruang sipil dan militer. Dengan demikian memperkuat dampak perang. Dalam penggunaan hukum untuk tujuan perang (*lawfare*), justru prinsip dan argumentasi hukum diarahkan kembali atau dimanipulasi dengan cara yang berorientasi sebagai pembenaran untuk memungkinkan daripada membatasi kekerasan militer. Di garis depan inovasi *lawfare*, misalnya, di antara pengacara militer Amerika Serikat dan Israel, hukum telah menjadi pengganda kekuatan yang bekerja di area abu-abu untuk memungkinkan kekerasan militer yang semakin merusak yang bergantung pada definisi dwiguna yang berubah-ubah. Ada banyak contoh *lawfare* dan instrumentalisasi dwiguna.¹⁹⁶

Dalam konteks ini, militerisasi teknologi (*militarization of technology*) menurut Mark Bromley dan Giovanna Maletta adalah istilah luas yang digunakan untuk merujuk pada serangkaian proses yang saling terkait yang mengikis perbedaan konvensional antara cara teknologi sipil dan peralatan militer serta keamanan diproduksi dan digunakan. Proses-proses ini mencakup penyebaran sistem intensif data untuk tujuan militer, yakni suatu situasi yang meletakkan perusahaan dan perusahaan rintisan yang telah mengembangkan teknologi infrastruktur komersial dan sipil memasuki sektor pertahanan dan penggunaan kembali serta adaptasi teknologi yang dikembangkan untuk digunakan di zona konflik untuk tujuan komersial.¹⁹⁷ Privacy International mengidentifikasi adanya fenomena kecenderungan pergeseran medan perang menuju ke kota-kota karena teknologi yang diandalkan setiap hari dimiliterisasi. Pada gilirannya, teknologi sipil yang

¹⁹⁴ Rushad Faridi, "Starlink in Gaza: Humanitarian Lifeline or Military Asset?," *The Daily Star*, 9 September 2025, <https://www.thedailystar.net/slow-reads/focus/news/starlink-gaza-humanitarian-lifeline-or-military-asset-3981756>.

¹⁹⁵ Jones, Mousamputri, dan Griffiths, "Dual Use as a Political Technology of Contemporary Military Violence."

¹⁹⁶ *ibid*

¹⁹⁷ Mark Bromley and Giovanna Maletta, *op.cit*

didorong oleh data dan kehidupan kemanusiaan bergerak ke medan perang. Perusahaan yang sama yang membangun piranti perang sedang berekspansi untuk menyediakan infrastruktur sipil, dan sebaliknya.¹⁹⁸ Menurut Privacy International fenomena ini terlihat dalam berbagai bentuk:¹⁹⁹

1. Negara-negara membawa teknologi militer ke pusat kota dengan menjalin kemitraan dengan industri teknologi pertahanan, yang disebut militerisasi ruang sipil (*militarisation of civilian spaces*);
2. Perusahaan teknologi sipil merambah medan perang, membawa serta data sipil, yang disebut militerisasi teknologi sipil (*militarisation of civilian tech*);
3. Perusahaan dan dana investasi swasta menggelontorkan sejumlah uang yang tak terbayangkan, menciptakan insentif untuk pengawasan dan perang, dan mengutamakan investor daripada rakyat, yang dikenal privatisasi teknologi militer (*privatisation of military tech*).

Situasi ini menggambarkan kompleks industri militer yang mempertemukan jalinan kepentingan yang luas yang dimiliki oleh militer, kontraktor pertahanan, dan pihak lain yang memiliki kepentingan dalam bisnis perang dan kekerasan bersenjata. Seiring dengan menyebarnya kepentingan finansial dan politik dalam perang di antara para pemimpin militer, kontraktor pertahanan, politisi, pelobi, universitas, dan lembaga pemikir, konsep modern kompleks industri militer menjadi semakin luas dan tidak terdefinisi dengan jelas. Pada sisi yang lain, industri pertahanan modern itu sendiri menjadi sulit untuk dibatasi, mencakup tentara bayaran hingga manufaktur senjata hingga layanan teknologi informasi. Dengan perusahaan seperti Boeing, Palantir, Oracle, dan lainnya yang melayani pasar militer dan sipil dengan teknologi dwiguna. Konsekuensi lebih jauh, industri pertahanan tampaknya semakin sulit dibedakan.²⁰⁰

Dampak lebih jauh, batasan antara militer dan sipil yang semakin kabur, maka terdapat risiko serius, maka pengembangan teknologi dalam satu konteks akan ditransfer ke konteks lain tanpa mempertimbangkan aturan keterlibatan yang berbeda. Terdapat risiko yang besar apabila kedua sektor tersebut terus dibiarkan memanfaatkan celah instrumen hukum dan pengawasan. Hal ini mengakibatkan eksploitasi yang lebih besar, konsentrasi kekuasaan yang lebih besar, dan mendorong militerisasi terus berlanjut.²⁰¹

Dalam kaitan ini, istilah industri militer (*military-industrial*) terlalu sempit untuk menggambarkan fenomena tersebut. Istilah ini tidak sepenuhnya membahas penguatan

¹⁹⁸ Privacy International, loc.cit

¹⁹⁹ ibid

²⁰⁰ Kaitlyn Church, "The Military-Industrial Complex: Why This Is of Importance to Action on Armed Violence and What It Has to Do with the Erosion of Civilian Protection," *Action on Armed Violence (AOAV)*, 14 Juli 2026, <https://aoav.org.uk/2026/the-military-industrial-complex-why-this-is-of-importance-to-action-on-armed-violence-and-what-it-has-to-do-with-the-erosion-of-civilian-protection/>.

²⁰¹ Privacy International, "Challenging the Militarisation of Tech."

politik dan budaya perang, yang dinormalisasi melalui segala hal mulai dari penelitian universitas yang disponsori pertahanan hingga perekrutan militer yang tertanam dalam budaya populer.²⁰² Sektor militer merupakan ranah di mana batas antara negara dan korporasi dapat menjadi sangat kabur. Dengan digitalisasi ekonomi dunia, tumpang tindih ini menjadi semakin kuat. Upaya mengendalikan jaringan digital dan *chokepoints* mengalir dari satu benua ke benua lain memungkinkan untuk mempersenjatai saling ketergantungan (*weaponizing interdependencies*) memberikan keuntungan besar atas musuh dan sekutu. Namun, hal ini hampir mustahil tanpa dukungan dari perusahaan Big Tech. Tanpa kehadiran Big Tech jaringan global hampir tidak dapat dipersenjatai.

Peran Big Tech semakin dominan karena perang kontemporer semakin menjadi digital. Ambil contoh, drone bertenaga kecerdasan artifisial yang dijual dengan harga kurang dari US\$100.000 dapat dengan mudah menghancurkan pesawat terbang atau tank yang harganya 100 kali lebih mahal. Sistem komunikasi *cloud* dan satelit canggih sangat penting untuk mengumpulkan informasi dan mencegah atau melaksanakan serangan fisik dan siber. Bahkan kinerja senjata konvensional, misalnya pesawat terbang, tank, sistem anti-pesawat sangat bergantung pada komponen digitalnya.²⁰³

Selama satu dekade terakhir, konsep yang sudah dikenal luas mengenai kompleks industri-militer yang dicetuskan oleh Presiden Dwight D. Eisenhower pada 1961 telah berkembang menjadi bentuk hibrida baru kompleks industri-militer-digital (*digital-military-industrial complex*). Varian ini berpusat pada perusahaan yang memiliki spesialisasi di bidang data, kecerdasan artifisial, dan platform digital, serta perusahaan rintisan (*startup*) yang secara sengaja memosisikan diri sebagai penyedia teknologi berorientasi pertahanan. Entitas-entitas ini menjalin kerja sama erat dengan militer Amerika Serikat dan kontraktor pertahanan konvensional untuk mempercepat digitalisasi serta transformasi berbasis kecerdasan pada kapabilitas militer. Varian digital ini dapat mendorong intervensi berskala besar oleh Amerika Serikat di luar negeri, yang berpotensi menjelma menjadi mesin perang baru (*new war machine*).²⁰⁴

Perusahaan raksasa pertahanan konvensional, seperti Lockheed Martin, Raytheon, Northrop Grumman, dan General Dynamics kini menghadapi persaingan sengit dari dua jenis pelaku industri digital. Kategori pertama mencakup perusahaan teknologi raksasa, seperti Microsoft, Amazon, Google, Oracle, HP, Dell, Motorola, IBM, dan lainnya yang banyak di antaranya telah memenangkan kontrak bernilai besar dari Pentagon untuk memasok perangkat lunak sistem canggih serta layanan cloud, data, dan kecerdasan artifisial. Kategori kedua terdiri dari perusahaan rintisan yang didukung modal ventura,

²⁰² Church, "The Military-Industrial Complex."

²⁰³ Coveri, Cozza, dan Guarascio, "Big Tech and the US Digital-Military-Industrial Complex."

²⁰⁴ Shi Bowei, "The Rise of the US 'Digital-Military-Industrial Complex,'" *China Daily*, 20 Oktober 2025, <https://www.chinadaily.com.cn/a/202510/20/WS68f599c6a310f735438b5e2d.html>.

sering kali didanai oleh investor Silicon Valley, yang berfokus pada kecerdasan artifisial, sistem otonom, teknologi penginderaan, serta sistem komando dan kendali berbasis jaringan yang dirancang khusus untuk kebutuhan militer dan intelijen. Perusahaan-perusahaan rintisan ini mengedepankan keamanan nasional sebagai atribut utama produk mereka dalam upaya meraih pangsa pasar pengadaan pertahanan Amerika Serikat.²⁰⁵

Dari perspektif perusahaan, terdapat keuntungan dalam memperluas aktivitas tersebut. Pertama, pada saat meningkatnya kekhawatiran tentang konflik global, khususnya Ukraina dan Timur Tengah dan persaingan kekuatan besar, beberapa eksekutif teknologi dan perusahaan mereka sebagai penjaga keamanan nasional Amerika Serikat. Kedua, ketika perusahaan-perusahaan teknologi besar memperluas kontrak mereka dengan Pentagon, hal itu memungkinkan untuk memanfaatkan sumber pendapatan yang sangat menguntungkan, dan terus berkembang tanpa henti.²⁰⁶ Pada akhir 2022, Pentagon mengumumkan kontrak senilai \$9 miliar untuk inisiatif Joint Warfighting Cloud Capability (JWCC) yang diberikan bersama kepada Microsoft, Google, Oracle, dan Amazon. Kesepakatan tersebut dengan jelas menunjukkan komitmen industri teknologi untuk bekerja sama dengan Pentagon. Kesepakatan ini menepis keraguan tentang apa yang disebut kesenjangan budaya antara Silicon Valley dan Washington. Tujuan program ini adalah untuk menyediakan layanan komputasi awan secepat misi, di semua tingkat klasifikasi, dari markas besar hingga ujung taktis. Meskipun protes karyawan yang berkelanjutan terhadap kontrak militer, seperti Project Nimbus, yakni kontrak komputasi awan Google dan Amazon dengan pemerintah Israel yang mencakup kemampuan pengenalan wajah, analisis video, dan analisis sentimen, para eksekutif perusahaan tetap melanjutkannya.²⁰⁷ Menurut Pelapor Khusus Francesca Albanese tentang Situasi HAM di wilayah Palestina yang diduduki sejak 1967 (Report of the Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967) menegaskan keterlibatan Microsoft, Amazon, dan Google termasuk di antara perusahaan-perusahaan besar yang diidentifikasi sebagai bagian dari *joint criminal enterprise* dalam membantu Israel melakukan genosida di Gaza.²⁰⁸ Perusahaan-perusahaan tersebut telah memperoleh keuntungan yang belum

²⁰⁵ Bowei, "The Rise of the US 'Digital-Military-Industrial Complex.'"

²⁰⁶ González, *How Big Tech and Silicon Valley Are Transforming the Military-Industrial Complex*.

²⁰⁷ González, *How Big Tech and Silicon Valley Are Transforming the Military-Industrial Complex*.

²⁰⁸ Francesca Albanese, *From Economy of Occupation to Economy of Genocide*, Report of the Special Rapporteur on the Situation of Human Rights in the Palestinian Territories Occupied since 1967, UN Doc. A/HRC/59/23 (United Nations, 30 Juni 2025), <https://www.ohchr.org/en/documents/country-reports/ahrc5923-report-special-rapporteur-situation-human-rights-palestinian>.

pernah terjadi sebelumnya dari pembantaian lebih dari 62.000 warga Palestina sejak Oktober 2023.²⁰⁹

Teknologi untuk genosida (Tech for Genocide) terus berkembang. Piranti kecerdasan artifisial yang lebih baru, yang dimodelkan pada platform generatif, seperti ChatGPT sedang dikembangkan oleh intelijen Israel untuk mempercepat surveilans, penuntutan, dan penangkapan. Eksperimen ini tidak terisolasi dan terbatas pada genosida di Gaza. Eksperimen ini diproyeksikan menjadi masa depan peperangan otomatis, yang dikembangkan bersama dan didukung oleh perusahaan teknologi besar Amerika Serikat. Peran Israel sebagai laboratorium imperialisme Amerika Serikat (*Israel's role as a laboratory for US imperialism*) yang menghubungkan semua ini. Setiap piranti pendudukan (*every tool of occupation*) yang diuji pada warga Palestina menjadi ekspor global. Piranti lunak kepolisian prediktif yang dirintis di Tepi Barat dijual kepada departemen kepolisian Amerika Serikat. Pos pemeriksaan biometrik yang diuji coba di Yerusalem Timur muncul di perbatasan Amerika Serikat-Meksiko. Surveilans kecerdasan artifisial yang diuji di Gaza dipasarkan kepada rezim otoriter di seluruh dunia. Bagi Big Tech, Israel adalah klien yang menguntungkan sekaligus tempat uji coba. Dengan menanamkan diri mereka dalam mesin militer Israel, Microsoft, Google, Amazon, dan Palantir bersama-sama mengembangkan teknologi penindasan yang dapat ditingkatkan dan dijual di seluruh dunia. Penghancuran Gaza bukan hanya menjadi proyek geopolitik, tetapi juga model bisnis. Perpaduan antara Big Tech dan military-industrial-surveillance complex telah sempurna. Israel menjadi salah satu garda terdepan proyek ini, tetapi cakupannya global. Dari Gaza hingga Ukraina, dari Baghdad hingga San Diego, perusahaan-perusahaan yang sama meraup keuntungan dari surveilans, penargetan, dan penindasan.²¹⁰

Dalam konteks ini, Craig Jones, Ichamati Mousamputri dan Mark Griffiths mendefinisikan wacana dan infrastruktur dwiguna (*dual use discourses and infrastructures*) sebagai jaringan diskursif, material, dan relasional yang menempatkan orang, tempat, dan benda dapat diidentifikasi sebagai militer dan sipil, serta proses pembuatan dan penghilangan perbedaan antara militer dan sipil. Dalam konteks ini pemisahan antara dunia militer

²⁰⁹ Sistem apartheid dan militer Israel membutuhkan kapasitas penyimpanan dan komputasi awan yang terus meningkat. Proyek komputasi awan pemerintah dan militer Israel yang dikenal sebagai Proyek Nimbus yang menggandeng Google dan Amazon dengan kontrak senilai \$1,2 miliar pada 2021 dirancang untuk memenuhi kebutuhan ini, Bahkan ketika komputasi awan internal militer Israel kelebihan beban pada Oktober 2023, Microsoft, Google, dan Amazon turun tangan untuk menyediakan teknologi awan dan AI yang sangat penting. Kepala komputer IDF, Kolonel Racheli Dembinsky menyatakan platform yang merupakan senjata untuk menggambarkan teknologi awan sebagai bagian dari kumpulan sistem yang digunakan IDF. Lihat, Progressive International, "UN Calls Out Google and Amazon for Abetting Gaza Genocide," 26 Agustus 2025, <https://progressive.international/wire/2025-08-26-un-calls-out-google-and-amazon-for-abetting-gaza-genocide/en/>.

²¹⁰ Bappa Sinha, "Big Tech's Deep Links With Genocide in Gaza," *NewsClick*, 6 Oktober 2025, <https://www.newsclick.in/big-techs-deep-links-genocide-gaza>.

dan dunia sipil dari dua sudut pandang yang berlawanan. *Pertama*, dalam perspektif kemanusiaan dan hukum untuk mengkodifikasi ruang sipil dengan cara yang melawan teknologi dwiguna.

Kedua, dalam instrumentalisasi dwiguna untuk melegitimasi kekerasan militer terhadap situs dan tubuh sipil. Di satu sisi, terutama dari perspektif HAM dan hukum internasional, terdapat upaya untuk membatasi ruang non-militer dari sasaran militer dengan tujuan melindungi nyawa warga sipil. Di sisi lain, terdapat pendekatan militer untuk mengaburkan batasan tersebut, seringkali dengan memusatkan klaim kombatan menggunakan warga sipil sebagai perisai manusia (*human shields*) dan objek dan tempat sipil dapat digunakan untuk tujuan militer.²¹¹

Pergeseran pusat kompleks industri militer ini mendorong para pemangku kepentingan memberikan perhatian atas beberapa hal:²¹²

1. Terdapat garis batas yang kabur antara teknologi sipil dan militer.

Fenomena semakin kaburnya batasan antara perusahaan teknologi dan sektor pertahanan. Perusahaan teknologi yang dulunya menjaga jarak dari keterlibatan militer kini menjadi aktor kunci. Ini termasuk perusahaan yang meninggalkan komitmen sebelumnya untuk menghindari produksi produk kecerdasan artifisial untuk tujuan militer. Konsep dwiguna (*dual use*) masih kurang terdefinisi dan penerapannya belum konsisten. Ambiguitas ini menyulitkan investor dan publik untuk mengevaluasi risiko yang terkait dengan produk teknologi yang digunakan dalam konteks militer.²¹³

2. Akuntabilitas dan tanggung jawab yang terbatas tetap menjadi masalah utama

²¹¹ Jones, Mousamputri, dan Griffiths, "Dual Use as a Political Technology of Contemporary Military Violence."

²¹² UN B-Tech Project, Heartland Initiative, Business & Human Rights Resource Centre, dan Open MIC, *Key Takeaways: Dual-Use Dominance When Every Innovation Has a Defense Application*, 26 Juli 2025, <https://www.ohchr.org/sites/default/files/documents/form/defense-application-key-takeaways-25-internet-governance-forum-side-event-dual-use-dominance-innovation-1-en.pdf>.

²¹³ Dalam kerangka hukum humaniter internasional, pembedaan tersebut lebih jelas, aset diklasifikasikan sebagai sipil atau militer berdasarkan penggunaannya, bukan berdasarkan desain atau niatnya. Gagasan tentang zona abu-abu hukum semestinya tidak dapat dipergunakan, sebaliknya kejelasan hukum harus banyak diadopsi oleh perusahaan dan investor ketika menilai peran dan tanggung jawab mereka, daripada mengandalkan asumsi netralitas. Beberapa perusahaan teknologi dengan sengaja mengejar kontrak dengan pemerintah yang banyak dikritik karena pelanggaran HAM. Banyak perusahaan setuju untuk melakukan penilaian dampak HAM, tetapi menghindari melakukannya dalam konteks militer. Hal ini mencerminkan kurangnya transparansi. Dengan tersedianya perangkat kecerdasan artifisial, intelijen sumber terbuka, dan pelaporan masyarakat sipil, perusahaan dapat melakukan uji tuntas yang lebih kuat di seluruh rantai nilai perusahaan dan diwajibkan untuk melakukan uji tuntas HAM yang lebih ketat ketika teknologi mereka digunakan di daerah yang terkena dampak konflik. Lihat, UN B-Tech Project et al., *Key Takeaways: Dual-Use Dominance When Every Innovation Has a Defense Application*.

Para pemangku kepentingan menggarisbawahi kurangnya akuntabilitas yang berarti bagi perusahaan teknologi yang akan menimbulkan risiko serius. Akuntabilitas menjadi masalah struktural yang meluas melampaui satu perusahaan karena risiko meluas menjangkau vendor pihak ketiga dan penyedia infrastruktur. Narasi geopolitik yang dominan, khususnya yang berfokus pada persaingan teknologi internasional, berkontribusi pada peningkatan toleransi risiko dalam lembaga pertahanan. Militer mungkin mengabaikan kerentanan atau terus maju dengan sistem yang tidak lolos tinjauan hukum. Transparansi yang minim mengenai kapan perusahaan yang mengumpulkan data sipil dapat menggunakannya kembali untuk melatih sistem AI yang berfokus pada militer, yang memiliki implikasi serius terhadap persetujuan dan privasi.²¹⁴

3. Perangkat uji tuntas konvensional (tradisional) tidak memadai untuk konteks ini

Pendekatan investor konvensional mungkin tidak sepenuhnya menangkap risiko yang ditimbulkan oleh teknologi multi-guna. Seiring perusahaan teknologi berekspansi ke sektor pertahanan, seringkali tanpa pemahaman yang cukup tentang tanggung jawab militer. Perangkat baru seperti kecerdasan artifisial dan infrastruktur komputasi awan seringkali berada di luar klasifikasi senjata konvensional. Upaya mendasarkan penilaian pada hukum humaniter internasional menawarkan landasan hukum dan etika yang lebih jelas tetapi membutuhkan keterlibatan investor secara aktif melampaui standar lingkungan, sosial, dan tata kelola (Environment, Social, and Governance);

4. Kepatuhan terhadap kontrol ekspor saja tidak cukup

Kepatuhan terhadap rezim kontrol ekspor tidak dapat dianggap sebagai uji tuntas yang memadai, khususnya dalam konteks teknologi multi-guna. Meskipun undang-undang ekspor senjata mencakup beberapa kasus terkait pertahanan, undang-undang tersebut digambarkan tidak dapat diandalkan untuk secara konsisten mengidentifikasi teknologi berisiko tinggi. Izin ekspor, seringkali mencerminkan aliansi politik daripada pertimbangan HAM;

5. Ke depan sejumlah langkah perlu diambil.

Upaya mengatasi risiko HAM yang terkait dengan teknologi multi-guna membutuhkan lebih dari sekadar prinsip-prinsip umum. Beberapa berpendapat menyatakan Prinsip-Prinsip Panduan PBB (UNGPs) sudah cukup, sementara

²¹⁴Sistem senjata atau teknologi dwiguna semakin meminimalkan peran manusia karena hanya sekedar menjalankan hasil yang telah ditentukan sebelumnya yang dihasilkan oleh kecerdasan artifisial. Pengurangan peran ini semakin memperumit struktur akuntabilitas. Lihat, UN B-Tech Project et al., *Key Takeaways: Dual-Use Dominance When Every Innovation Has a Defense Application*.

yang lain menganjurkan panduan tambahan yang membahas bagaimana kerangka kerja tersebut diterapkan pada konteks penggunaan ganda.

Titik tuju atensi tersebut dapat diletakkan pada tiga isu tata kelola teknologi dwiguna. *Pertama* perbedaan kesadaran tantangan tata kelola tiga domain teknologi dwiguna yang berbeda. Misalnya, meskipun ada kesepakatan umum secara internasional tentang perlunya membatasi akses teknologi pengembangan senjata nuklir, namun tidak ada konsensus seperti itu pada domain biologi dan teknologi informasi. Bahkan, dalam penelitian bioteknologi, ada penentangan yang cukup besar dari komunitas ilmu biologi terhadap setiap upaya untuk membatasi akses atau penyebaran temuan penelitian, termasuk informasi yang dapat menyebabkan kerugian besar. Sementara, di arena teknologi informasi, sebagian besar diabaikan. Dalam beberapa kasus, secara rutin teknologi informasi menyusup ke jaringan satu sama lain untuk mendapatkan intelijen dan informasi jaringan, termasuk identifikasi kerentanan yang memungkinkan eksploitasi di masa depan.

Kedua, model tata kelola yang efektif mengasumsikan kemampuan untuk mengidentifikasi dan menghukum pelanggar ketentuannya. Meskipun ada beberapa tingkat atribusi yang mungkin dilakukan di bidang nuklir, namun atribusi di bidang biologi jauh lebih kompleks dan mungkin secara praktis tidak mungkin dilakukan dalam kasus teknologi informasi. Dan *ketiga*, masalah penegakan hukum yang membingungkan bahkan bidang piranti dwiguna yang paling mudah dipahami sekalipun.²¹⁵

Perubahan tata kelola teknologi dwiguna perlu diletakkan dalam konteks fusi antara militer dan sipil dalam konteks revolusi industri keempat. Fusi antara militer dan sipil ini menurut Yoram Evron dan Richard A. Bitzinger dilandasi argumentasi:

1. Teknologi yang terkait dengan Revolusi Industri keempat yang sedang berkembang semakin dipahami sebagai penentu dasar efektivitas dan keunggulan militer di masa depan. Seperti Revolusi Industri ketiga, Revolusi industri keempat sebagian besar didasarkan pada teknologi digital, dan khususnya teknologi informasi, seperti mikroelektronika, komputasi, perangkat lunak, dan sejenisnya. Namun demikian, revolusi industri keempat melampaui revolusi industri ketiga. Revolusi industri keempat mengarah pada pengumpulan, penyimpanan, dan pengolahan data, tetapi dengan skala yang jauh lebih besar daripada yang pernah dibayangkan pada saat pengembangan revolusi industri ketiga. Seperti halnya revolusi industri ketiga, revolusi industri keempat tentang komunikasi dan jaringan, tetapi dalam skala, kompleksitas, dan intensitas yang jauh lebih besar baik dalam hal konektivitas, berbagi, dan kebersamaan. Di atas segalanya, revolusi industri keempat adalah tentang daya pemrosesan, kapasitas penyimpanan, dan akses tak terbatas ke

²¹⁵ Rosner, "Preface."

pengetahuan yang belum pernah terjadi sebelumnya, yang menghubungkan orang dan benda sambil menghasilkan perpaduan teknologi yang mengaburkan batas antara ranah fisik, digital, dan biologis;

2. Upaya memanfaatkan potensi teknologi revolusi industri keempat mensyaratkan militer menciptakan bentuk baru kerja sama sipil-militer dalam sains dan teknologi. Sejak akhir tahun 2010-an, strategi ini dikenal sebagai fusi militer-sipil (*military-civil fusion*) suatu bentuk kerja sama militer-sipil yang semakin diakui sebagai mekanisme utama untuk asimilasi teknologi revolusi industri keempat oleh militer. Fusi militer-sipil menguat pasca Perang Dingin ketika sektor sipil mengambil alih posisi sektor militer sebagai sumber teknologi inovatif yang paling penting, Fusi militer-sipil berkaitan dengan menyediakan inovasi teknologi kepada militer yang awalnya berasal dari sektor komersial. Fusi militer-sipil kontemporer berfokus pada teknologi komersial mutakhir, terutama teknologi revolusi industri keempat yang kemudian dapat diadaptasi dan diintegrasikan ke dalam sistem militer dan mampu memberikan kemajuan signifikan dalam kemampuan militer. Pada saat yang sama, fusi militer-sipil lebih dari sekadar menemukan dan mengasimilasi teknologi sipil. Hal ini juga berkaitan dengan merancang strategi dan inisiatif untuk menemukan teknologi dan produsen sipil yang memadai, kemudian memanfaatkannya untuk proyek penelitian dan pengembangan militer, melibatkan militer dalam kolaborasi penelitian dan pengembangan dengan entitas sipil.

Hal ini dapat diartikan dunia siber telah membentuk kembali fondasi konseptual dan kelembagaan hubungan sipil-militer. Menurut Isabella Neumann dunia siber telah menggoyahkan otoritas, memecah koordinasi, meningkatkan politisasi, dan memperluas pengaruh sektor swasta, memperdalam ketergantungan negara pada kemampuan sipil. Di dalam organisasi militer, hierarki dikonfigurasi ulang di sekitar keahlian teknis, menekan otoritas dan mengintensifkan persaingan. Di luar militer, kerentanan infrastruktur bersama mengikat ranah sipil dan militer, sementara platform digital membentuk kembali legitimasi dan kepercayaan publik. Pembungkahan dunia siber sebagai domain peperangan semakin memperluas pengaruh militer ke dalam tata kelola sipil (*civilian governance*).²¹⁶ Selanjutnya, Isabella Neumann mengidentifikasi tiga simpulan untuk menelisik hubungan militer -sipil dalam konteks dunia maya:²¹⁷

1. Dunia siber beroperasi sebagai kondisi transversal yang meresap ke dalam berbagai dimensi hubungan sipil-militer, mengubah baik distribusi kemampuan maupun lokasi dan karakter otoritas itu sendiri. Oleh karena itu, kekhasan dunia siber terletak pada bagaimana cara mengatur ulang interaksi di seluruh dimensi inti hubungan sipil-militer. Bahkan perkembangan di satu domain bergema di

²¹⁶ Neumann, "It Is Complicated: Cyber into the Civil-Military Relationship."

²¹⁷ Neumann, "It Is Complicated: Cyber into the Civil-Military Relationship."

domain lain dalam dunia siber akan menghasilkan lingkaran umpan balik rekursif yang mengaburkan perbedaan dan mendekonstruksi pemahaman linier atau terkotak-kotak tentang hubungan sipil-militer;²¹⁸

2. Pertimbangan mengenai militerisasi di ranah siber akan dibarengi kontrol sipil serta beralihnya keahlian ke pihak sipil dan sektor swast. Hal ini memunculkan tantangan terhadap supremasi sipil dan demokrasi karena kontrol atas kapabilitas krusial bersifat terfragmentasi dan tidak dapat dengan mudah dikonsolidasikan hanya di dalam institusi militer. Militerisasi konvensional melibatkan perluasan logika, personel, atau piranti militer secara bertahap ke dalam ranah sipil. Namun, di ranah siber, militerisasi mengambil bentuk yang berbeda. Aktor militer memperluas jangkauan ke dalam lingkungan informasi dan infrastruktur digital. Akibatnya, pola-pola klasik seperti komando terpusat, disiplin hierarkis, dan kontrol atas instrumen kekuasaan negara tidak dapat dengan mudah direplikasi di ranah siber. Kontrol sipil mungkin terpengaruh oleh teknologi siber, karena kapabilitas siber militer yang mengakar kuat dan bertahan melampaui pergantian rezim;
3. Dunia siber mengungkap ketegangan mendasar antara logika institusional sipil-militer yang mapan dan persyaratan operasional domain tersebut. Tata kelola yang efektif membutuhkan keahlian yang terdistribusi, pertukaran informasi yang cepat, dan kolaborasi lintas sektor yang berkelanjutan sehingga bentuk organisasi standar struktur komando vertikal, demarkasi sipil-militer yang kaku, sistem intelijen yang terkotak-kotak, jangka waktu akuisisi multi-tahun, dan proses perencanaan strategis yang hierarkis kurang sesuai karakteristik dunia siber. Dinamika ini menunjukkan implikasi yang lebih luas. Kerangka kerja hubungan sipil-militer yang ada kesulitan untuk menjelaskan bentuk-bentuk interaksi yang didefinisikan oleh saling ketergantungan, simultanitas, dan difusi. Oleh karena itu, hal ini menuntut pemikiran ulang tentang landasan konseptual untuk memahami hubungan sipil-militer.

²¹⁸ Tuntutan operasional dunia maya, baik keahlian teknis, fleksibilitas, dan koordinasi yang berkesinambungan menarik aktor sipil dan militer ke dalam interaksi yang lebih dekat, mengaburkan batas antara peran politik dan militer. Secara eksternal, hal ini membuka ruang bagi aktor non-negara, baik perusahaan swasta, komunitas teknis, dan entitas hibrida untuk berfungsi sebagai simpul otoritas dalam jaringan tata kelola. Hubungan militer-sipil, pada saat yang sama, dibentuk kembali melalui kerentanan bersama dan kontestasi simbolik. Secara umum, otoritas menjadi mudah dipahami sebagian, tetapi buram secara keseluruhan sehingga dapat menghambat mekanisme pengawasan dan akuntabilitas konvensional. Dalam organisasi militer, siber memicu serangkaian efek kelembagaan akibat dunia siber meratakan hierarki dengan menggeser kapasitas analitis dan pengambilan keputusan dari jajaran senior. Oleh karena itu, kekhasan dunia siber terletak pada bagaimana dunia siber mengatur ulang interaksi di seluruh dimensi inti hubungan sipil-militer. Lihat, Neumann, "It Is Complicated: Cyber into the Civil–Military Relationship."

Berdasarkan ketiga simpulan tersebut Isabella Neumann mengidentifikasi kategori tematik dari perspektif keamanan siber yang melintasi pilar-pilar hubungan sipil-militer:²¹⁹

Kategori Tematik	Kasus Representatif
Pilar Tradisional	
§ Kudeta militer	-
§ Transisi demokrasi	-
§ Kontrol sipil	Operasi zona abu-abu yang mengaburkan batas antara perdamaian dan konflik; destabilisasi struktur otoritas tradisional; kegagalan koordinasi antara lembaga sipil dan komando siber militer; peningkatan risiko politisasi; pengaruh aktor sektor swasta terhadap pertahanan siber nasional.
Pilar Kontemporer	
§ Aktor non-negara	Krisis hibrida dan ancaman multidomain; ketergantungan negara pada kemampuan siber sipil dan sektor swasta; proliferasi piranti siber ofensif oleh kelompok proksi; perusahaan teknologi swasta yang beroperasi sebagai simpul penting dalam pertahanan siber nasional
§ Studi Organisasi Militer	Restrukturisasi hierarki komando berdasarkan keahlian teknis; kompresi wewenang seiring meningkatnya signifikansi operasional personel junior; persaingan antar organisasi atas kepemilikan misi siber; adaptasi budaya; bias kognitif dalam pengambilan keputusan pencegahan siber; tantangan perekrutan dan retensi di pasar tenaga kerja teknis yang kompetitif.
§ Hubungan militer-masyarakat	Kerentanan bersama infrastruktur sipil dan militer terhadap serangan siber; penggunaan platform digital oleh militer untuk legitimasi dan manajemen narasi; erosi kepercayaan publik setelah pelanggaran data tingkat tinggi; kaburnya perbedaan antara target sipil dan militer dalam konflik siber.
§ Politisasi	Pembingkaian militer terhadap dunia siber sebagai domain peperangan; konsep doktrin yang memperluas relevansi militer ke ranah pemerintahan sipil; platform siber yang beririsan dengan politik elektoral dan debat politik; ambiguitas hukum dan konseptual yang menciptakan ruang bagi interpretasi militer.
§ Militerisasi	Pembentukan komando siber khusus; normalisasi keterlibatan yang berkesinambungan dan doktrin pertahanan maju;

²¹⁹Militerisasi di domain siber, bila diletakkan dengan elemen kontrol sipil dan relokasi keahlian ke aktor sipil dan sektor swasta, maka hal ini dapat membantu menjelaskan mengapa beberapa pilar konvensional bidang ini, seperti pembangkitan militer dan transisi demokrasi, memerlukan analisis terpisah. Hal ini menunjukkan meskipun kehadiran militer dapat meluas di domain siber, penyebaran keahlian dan kemampuan di antara aktor non-militer, maka pembangkitan militer menjadi tidak mungkin, karena kontrol atas kemampuan terfragmentasi dan tidak dapat dengan mudah dikonsolidasikan hanya dalam institusi militer saja. Ini menciptakan dinamika paradoks, jejak operasional militer meluas ke ranah siber tetapi otoritas relatifnya atas domain siber tidak memungkinkan untuk dikontrol sepenuhnya. Lihat ibid

	persaingan birokrasi untuk sumber daya siber dan prestise kelembagaan; perluasan logika militer ke dalam pelindungan infrastruktur sipil.
--	---

Apabila menelisik pilar dan kasus yang merepresentasikan setiap pilar kontemporer relasi militer-sipil dalam konteks dunia siber, maka isu tata kelola menjadi penting untuk mengurangi risiko dari teknologi penggunaan ganda. Dengan demikian tujuan dari tata kelola penggunaan teknologi dwiguna menurut Elisa D. Harris dapat diletakkan dalam konsep umum, seperti nonproliferasi, keamanan, dan keselamatan. Atau tujuan tata kelola ini difokuskan pada tujuan yang lebih spesifik, termasuk:

1. Mencegah teknologi dwiguna dikembangkan dan digunakan untuk tujuan yang bermusuhan;
2. Mengendalikan akses terhadap material, peralatan, dan informasi atau pengetahuan yang terkait dengan teknologi dwiguna; dan
3. Mempromosikan penanganan dan penggunaan material, peralatan, atau informasi yang terkait dengan teknologi dwiguna secara aman dan terjamin.

6.1. Palestina sebagai Laboratorium Penggunaan Teknologi Dwiguna dan Relevansinya dalam Konteks Indonesia: Praktik Politik Mis-apropriasi HAM

Charles Santiago ketua bersama ASEAN Parliamentarians for Human Rights (APHR) mengkritisi pembelian dan penggunaan piranti spyware yang sangat invasif dari perusahaan surveilans yang berbasis di Israel untuk memata-matai kelompok-kelompok kritis mengekspresikan hak ekspresionalnya. Lebih jauh, Charles Santiago menyatakan adanya kesenjangan antara klaim publik mereka dan tindakan penindasan yang sebenarnya.²²⁰

“Kami sangat terkejut bahwa meskipun pemerintah Indonesia telah lama mendukung rakyat Palestina, mereka telah membeli dan menggunakan spyware yang telah digunakan untuk melawan pembela hak asasi manusia dan jurnalis di Palestina, serta di seluruh dunia,

Ini adalah puncak kemunafikan untuk secara terbuka mengutuk Israel sementara pada saat yang sama secara diam-diam menggunakan taktik rezim Israel terhadap warga negara Indonesia sendiri.”

Pernyataan ini menunjukkan adanya indikasi praktik kemunafikan (*hypocrisy*) suatu negara dalam melaksanakan kewajiban HAM. Praktik kemunafikan mengaku patuh pada aturan sembari sibuk melanggarnya yang umum terjadi dalam sistem internasional,

²²⁰ APHR, “Indonesia Must Halt the Import and Use of Highly Invasive Spyware.”

di mana aturan sering kali dipatuhi meskipun dilanggar.²²¹ Kate Cronin-Furman menginisiasi kepatuhan semu (*quasi-compliance*) untuk menggambarkan perilaku yang jelas dimotivasi oleh tekanan untuk mematuhi suatu aturan tetapi tidak dilakukan dengan maksud untuk benar-benar memenuhi persyaratan aturan tersebut. Kepatuhan semu merupakan semacam mekanisme satu arah, yang menetapkan batas bawah baru untuk kinerja negara dalam kewajiban HAM. Dengan kata lain, sementara tekanan HAM internasional dapat secara terukur memengaruhi perilaku negara-negara represif, tekanan tersebut tidak dapat memunculkan kepatuhan terhadap standar internasional tanpa adanya motivasi domestik untuk mematuhi.²²²

Pemerintah Indonesia sampai saat ini belum menandatangani mekanisme tata kelola global intrusi siber komersial menjadi indikasi ketiadaan komitmen politik (*political will*) untuk terlibat dalam upaya memerangi penyalahgunaan *spyware*. Indonesia tidak hadir dalam Proses Pall Mall maupun pernyataan bersama (*joint statement*) yang dihasilkan Konferensi Tingkat Tinggi (KTT) Demokrasi Ketiga di Seoul, Korea Selatan. KTT Ketiga untuk Demokrasi, pada 18 Maret 2024 di Seoul dengan tema Menggerakkan Aksi Multi-Pemangku Kepentingan untuk Memerangi Penyalahgunaan *Spyware* Komersial. (Galvanizing Multi-Stakeholder Action to Combat the Misuse of Commercial Spyware). KTT ini menghasilkan pernyataan bersama tentang penanggulangan proliferasi dan penyalahgunaan *spyware* komersial. Pernyataan tersebut, yang awalnya diumumkan pada Maret 2023, kini telah ditandatangani oleh beberapa negara, termasuk Amerika Serikat, Jepang, Korea Selatan, dan Finlandia yang juga merupakan anggota Proses Pall Mall. Pada Februari 2024 awalnya diinisiasi oleh Inggris dan Perancis, diselenggarakan dialog multi-pemangku kepentingan terpisah yang dirancang untuk memerangi penyalahgunaan dan penyebaran piranti surveilans komersial. Proses ini muncul sebagai tanggapan terhadap meningkatnya kekhawatiran tentang penyalahgunaan piranti *spyware* komersial, seperti piranti *spyware* Pegasus yang dikembangkan oleh NSO Group Israel.²²³ Meskipun kelompok negara yang terlibat beragam, Pemerintah Indonesia belum bergabung dalam proses tersebut atau mengomentari keberadaannya. Ketidakhadiran Pemerintah Indonesia menunjukkan politik domestik dan identitas global mengenai penggunaan piranti *spyware* komersial.²²⁴

²²¹ Kate Cronin-Furman, *Hypocrisy and Human Rights: Resisting Accountability for Mass Atrocities* (Ithaca, NY: Cornell University Press, 2022).

²²² Cronin-Furman, *Hypocrisy and Human Rights*.

²²³ Pengungkapan skandal Pegasus dan penyalahgunaan piranti *spyware* komersial lainnya memicu reaksi keras dari pemerintah dan industri, termasuk melalui Proses Pall Mall. Hingga saat ini, proses tersebut mencakup perwakilan dari Uni Afrika, Australia, Dewan Kerja Sama Teluk (Gulf Cooperation Council), Malaysia, Jepang, Singapura, AS, dan Swiss. Gatra Priyandita dan Arindrajit Basu, "Why Haven't India and Indonesia Signed Up for Anti-Spyware Dialogue?" *Royal United Services Institute*, 10 April 2024, <https://www.rusi.org/explore-our-research/publications/commentary/why-havent-india-and-indonesia-signed-anti-spyware-dialogue>.

²²⁴ Priyandita dan Basu, "Why Haven't India and Indonesia Signed Up for Anti-Spyware Dialogue."

Indonesia masih menempatkan kedaulatan sebagai prinsip utama untuk memperlihatkan pelaksanaan kebijakan luar negeri dan domestik sebagai bagian dari otonomi negara. Upaya menjaga ruang kebijakan domestik untuk mengejar tujuan keamanan, ekonomi, dan pembangunan merupakan tujuan penting dari upaya diplomatik. Meskipun Pemerintah Indonesia terlibat dengan mekanisme tata kelola formal dan informal di bidang siber dan teknologi kritis, persetujuan Pemerintah Indonesia bukanlah otomatis tetapi didasarkan pada kekhawatiran domestik dan konteks geopolitik yang spesifik. Indonesia relatif memiliki kedudukan global dan kemampuan material untuk menolak tekanan bergabung dengan mekanisme tata kelola.²²⁵

Terdapat tiga faktor yang mendasari mengapa Pemerintah Indonesia masih belum memiliki kemauan politik dan terkesan menjauh dari Proses Pall Mall dan diplomasi *spyware*.²²⁶

1. Bergabung dengan Proses Pall Mall mungkin bukan prioritas diplomatik langsung atau sesuai untuk Pemerintah Indonesia. Upaya untuk memerangi *spyware* tentu bukan prioritas utama dalam agenda diplomatik Indonesia. Dalam beberapa tahun terakhir, diplomasi siber Indonesia sebagian besar berfokus pada memerangi terorisme online, mengadvokasi netralitas teknologi dan kedaulatan data, serta menyerukan lebih banyak dukungan untuk pembangunan kapasitas siber di Global South. Meskipun surveilans siber telah muncul sebagai masalah keamanan nasional sejak pengungkapan Edward Snowden tahun 2013, masalah ini belum menonjol dalam agenda diplomatik;
2. Terdapat argumentasi yang lebih substansial karena diduga Indonesia menggunakan *spyware* dalam operasi siber domestik dan internasional. Hal ini menjadi faktor yang menyebabkan Indonesia belum mengambil posisi yang jelas mengenai pembatasan kemampuan intrusi *spyware* komersial. Otoritas Indonesia diduga menggunakan *spyware* komersial untuk memata-matai pemimpin oposisi dan aktivis;²²⁷
3. Dari segi moral, Pemerintah Indonesia tidak memandang surveilans demi kepentingan keamanan nasional sebagai tindakan negara yang tidak sah. Produk kebijakan Pemerintah Indonesia, baik legislasi maupun regulasi memprioritaskan pembangunan atau masalah keamanan internal daripada melawan surveilans. Arah kebijakan memperlihatkan kehendak Pemerintah Indonesia untuk mempertahankan keberadaan China yang berkesinambungan sebagai

²²⁵ Priyandita dan Basu, "Why Haven't India and Indonesia Signed Up for Anti-Spyware Dialogue."

²²⁶ Priyandita dan Basu, "Why Haven't India and Indonesia Signed Up for Anti-Spyware Dialogue."

²²⁷ Lihat Amnesty International, *A Web of Surveillance*.

perimeter teknologi Indonesia meskipun ada ketidakpercayaan strategis antara kedua negara.

Hal ini menunjukkan cakupan banyak sistem surveilans mengikuti lintasan yang jelas: *pertama*, berfungsi sebagai sarana untuk mengendalikan orang-orang dari Global South melalui perang dan kontrol perbatasan yang kejam. *Kedua*, berfungsi untuk menekan perbedaan pendapat di dalam negeri terhadap orang-orang yang berbicara menentang kebijakan. Ambil contoh, drone MQ-9 Predator/Reaper (surveilans dan serangan) milik General Atomics, telah meluas misinya dari militer, ke surveilans perbatasan Amerika Serikat, dan akhirnya ke surveilans domestik terhadap mereka yang menentang Immigration and Customs Enforcement (ICE) meskipun juga digunakan pada tahun 2020 untuk memata-matai para demonstran setelah pembunuhan George Floyd. Contoh lain dari teknologi militer yang digunakan terhadap penduduk domestik termasuk X10 buatan perusahaan rintisan Amerika Serikat Skydio yang telah teruji di medan perang, yang telah dikerahkan di wilayah domestik untuk memantau mereka yang berorganisasi melawan ICE, genosida Israel, dan pemerintahan Donald Trump. Di Eropa, Penjaga Pantai Yunani dilaporkan menggunakan persediaan drone militer Heron buatan Israel (diproduksi oleh Israel Aerospace Industries) untuk mengganggu misi Armada Kebebasan Gaza saat mereka mencoba mengirimkan bantuan ke Jalur Gaza.²²⁸

Greg Grandin, berpendapat Washington secara tradisional memandang Amerika Latin sebagai bengkel atau tempat pelatihan (workshop) sebagai tempat berkumpulnya kembali Amerika Serikat selama periode pengurangan kekuatan (*periods of retrenchment*) dan menguji cara-cara baru untuk mengendalikan negara-negara tetangganya.²²⁹ Sementara itu, Palestina menjadi bengkel bagi Israel yang menempatkan Palestina dianggap sebagai wilayah di depan pintunya yang menyediakan jutaan orang yang tertindas sebagai laboratorium untuk metode dominasi yang paling tepat dan berhasil. Israel sebagai model etnonasionalis ideal bergantung pada kemampuannya untuk mengkomersialkan pesan ini. Meskipun beberapa negara menginginkan senjata atau teknologi Israel hanya untuk memata-matai atau mengganggu perilaku pembangkang dan tidak tertarik untuk membangun entitas etnoreligius mereka sendiri, banyak negara lain mempercayai mitos tentang supremasi rasial Israel dan ingin menirunya di negara mereka sendiri. Industri pertahanan Israel tidak bermoral karena begitulah cara pertumbuhannya. Israel akan menjual kepada siapa pun kecuali musuh resmi seperti Korea Utara, Iran, atau Suriah.²³⁰

²²⁸ Corporate Watch, "What's Driving the Militarisation of Tech."

²²⁹ Greg Grandin Sejarahawan pemenang Hadiah Pulitzer, dalam bukunya yang terkenal tahun 2006, *Empire's Workshop: Latin America, the United States, and the Making of an Imperial Republic*. Lihat, Antony Loewenstein, *The Palestine Laboratory: How Israel Exports the Technology of Occupation Around the World* (London: Verso, 2023).

²³⁰ Loewenstein, *The Palestine Laboratory*.

Saat ini, penduduk Gaza ditempatkan dalam eksperimen kontrol paksa di mana teknologi dan teknik terbaru diuji. Laboratorium Palestina hanya dapat berkembang jika cukup banyak negara yang percaya pada premis dasarnya. Tidak mengherankan bahwa rezim represif ingin meniru penindasan Israel, menggunakan teknologi Israel untuk menindas penduduk mereka sendiri yang tidak diinginkan atau memberontak,²³¹ Palestina yang menjadi laboratorium milik Israel berkembang pesat di tengah gangguan dan kekerasan global. Krisis iklim yang memburuk akan menguntungkan sektor pertahanan Israel di masa depan, sementara negara-negara tidak menanggapi dengan tindakan aktif untuk mengurangi dampak kenaikan suhu. Secara praktis, ini berarti tembok yang lebih tinggi dan perbatasan yang lebih ketat, surveilans pengungsi yang lebih ketat, pengenalan wajah, drone, pagar pintar, dan basis data biometrik. Pada tahun 2025, kompleks industri surveilans perbatasan diperkirakan bernilai US\$68 miliar, dan perusahaan Israel seperti Elbit dijamin akan menjadi salah satu penerima manfaat utama.²³²

Pada tahun 2020, Dewan HAM PBB merilis daftar perusahaan, lokal dan asing, yang beroperasi di permukiman ilegal Tepi Barat dan Yerusalem Timur. Daftar tersebut termasuk Airbnb, Booking.com, Expedia, JCB, TripAdvisor, dan Motorola Solutions. Tak satu pun dari perusahaan-perusahaan ini berhenti beroperasi di sana karena hampir tidak ada tekanan publik atau politik untuk melakukannya.²³³

Laporan Pelapor Khusus tentang situasi HAM di wilayah Palestina yang diduduki sejak 1967 (Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967) Francesca Albanese memperkuat fakta penggunaan teknologi dwiguna nampak pada pendudukan Palestina oleh Israel. menyatakan teknologi sipil telah lama berfungsi sebagai perangkat dwiguna pendudukan kolonial pemukim. Operasi militer Israel sangat bergantung pada perangkat dari produsen global terkemuka untuk mengusir warga Palestina dari tanah mereka, menghancurkan rumah, bangunan publik,

²³¹ Israel mendambakan persetujuan Barat untuk sepenuhnya mewujudkan potensi diplomatik dan militernya. Selain Amerika Serikat, Jerman bisa dibilang merupakan hadiah terbesar dari semuanya. Israel membantu Jerman memulihkan citranya yang hancur setelah Perang Dunia II, sementara Berlin memberikan legitimasi kepada negara yang secara brutal menduduki Palestina yang dianggap bukan rakyat di mata pemerintah Jerman. Pembelian piranti pertahanan Israel dalam jumlah yang semakin meningkat oleh Jerman hanyalah salah satu cara untuk menebus kesalahan sejarahnya. Lihat Loewenstein, *The Palestine Laboratory*.

²³² Loewenstein, *The Palestine Laboratory*,

²³³ Semakin banyak investor institusional mulai menarik investasi dari perusahaan-perusahaan Israel, dengan alasan kekhawatiran atas keterlibatan dalam pelanggaran HAM oleh Israel. KLP, dana pensiun terbesar Norwegia dengan aset senilai US\$95 miliar, menarik investasi dari enam belas perusahaan pada tahun 2021 karena kontribusi risiko yang tidak dapat diterima terhadap pelanggaran HAM di permukiman Tepi Barat. Pada tahun yang sama, New Zealand Super Fund menjual US\$6,5 juta dari kepemilikannya di lima bank Israel, dengan alasan bukti kredibel bahwa perusahaan-perusahaan yang dikeluarkan tersebut menyediakan pembiayaan proyek untuk pembangunan permukiman ilegal Israel. Dengan demikian, keadaan mungkin berbalik. Pada tahun 2021, situs web Responsible Investor menemukan bahwa 67 persen manajer investasi berpikir bahwa HAM akan segera menjadi pertimbangan investasi utama, tidak jauh berbeda dengan sentralitas perubahan iklim saat ini. Lihat, Loewenstein, *The Palestine Laboratory*,

lahan pertanian, jalan, dan infrastruktur vital lainnya. Sejak Oktober 2023, mesin-mesin ini telah menjadi bagian integral dari kerusakan dan penghancuran 70 persen bangunan dan 81 persen lahan pertanian di Gaza.²³⁴ Francesca Albanese selanjutnya menyatakan dalam laporan tersebut:²³⁵

Penindasan terhadap warga Palestina semakin terotomatisasi, dengan keberadaan perusahaan teknologi yang menyediakan infrastruktur dwifungsi untuk mengintegrasikan pengumpulan data massal dan pengawasan, sekaligus mengambil keuntungan dari lahan uji coba unik untuk teknologi militer yang ditawarkan oleh wilayah Palestina yang diduduki. Didorong oleh raksasa teknologi Amerika Serikat yang mendirikan anak perusahaan dan pusat penelitian dan pengembangan di Israel, klaim Israel tentang kebutuhan keamanan telah memicu perkembangan yang belum pernah terjadi sebelumnya dalam layanan pemenjaraan dan pengawasan, mulai dari jaringan televisi sirkuit tertutup (CCTV), pengawasan biometrik, jaringan pos pemeriksaan teknologi canggih, “*smart walls*” dan surveilans drone hingga komputasi awan, kecerdasan artifisial dan analitik data yang mendukung personel militer di lapangan.

Laporan tersebut juga mengidentifikasi pengembangan mengembangkan sistem kecerdasan artifisial yang dikembangkan militer Israel, seperti “Lavender”, “Gospel”, dan “Where’s Daddy?”. Teknologi digunakan memproses data dan menghasilkan daftar target. Pengembangan teknologi ini telah mengubah peperangan modern dan menggambarkan dwiguna kecerdasan artifisial.²³⁶

Pelapor Khusus Francesca Albanese berpendapat bahwa ekonomi pendudukan Israel (*Israel’s economy of occupation*) telah berubah menjadi ekonomi genosida (*economy of genocide*) dan transformasi ini didukung tidak hanya oleh negara tetapi juga oleh perusahaan teknologi global. Laporan tersebut menyoroti bagaimana perusahaan yang menyediakan infrastruktur cloud, sistem kecerdasan buatan, dan analitik data kepada militer dan dinas intelijen Israel telah menjadi komponen integral dari kebijakan

²³⁴ Albanese, *From Economy of Occupation to Economy of Genocide*.

²³⁵ Albanese, *From Economy of Occupation to Economy of Genocide*.

²³⁶ Palantir telah menyediakan teknologi kepolisian prediktif otomatis, infrastruktur pertahanan inti untuk pembangunan dan penyebaran perangkat lunak militer yang cepat dan berskala besar, serta Platform Kecerdasan Artifisial yang memungkinkan integrasi data medan perang secara real-time untuk pengambilan keputusan otomatis. Pada Januari 2024, Palantir mengumumkan kemitraan strategis baru dengan Israel dan mengadakan rapat dewan di Tel Aviv sebagai bentuk solidaritas. Pada April 2025, CEO Palantir menanggapi tuduhan Palantir telah membunuh warga Palestina di Gaza dengan mengatakan, “sebagian besar teroris, itu benar. Hal ini menunjukkan pengetahuan dan tujuan tingkat eksekutif terkait penggunaan kekuatan yang melanggar hukum oleh Israel dan kegagalan untuk mencegah tindakan tersebut atau menarik keterlibatan. Lihat, Albanese, *From Economy of Occupation to Economy of Genocide*.

pengusiran dan penghancuran.²³⁷ Proses ini di era digital saat ini digambarkan Sara Roy sebagai kompleks digital-militer *kolonial* (*colonial digital–military complex*) yang didukung oleh partisipasi aktif korporasi global. Proses ini mengungkapkan bahwa kolonialisme digital berfungsi bukan hanya sebagai fenomena teknis atau ekonomi semata, tetapi sebagai bentuk dominasi yang dilegitimasi secara internasional. Tatanan kolonial digital Israel atas Palestina dibangun di atas tiga lapisan fundamental: infrastruktur, surveilans, dan narasi.²³⁸

Perusahaan seperti Palantir Technologies, melalui piranti kecerdasan artifisial menyediakan penargetan presisi dan telah membunuh warga sipil secara massal serta mengubah peperangan menjadi kampanye pemusnahan yang terencana dan sistematis dengan sedikit pengawasan manusia. Keterlibatan raksasa teknologi ini di Israel mendahului perjanjian formalnya selama bertahun-tahun. Palantir telah aktif di Israel sejak 2015, waktu perjanjian strategis, yang disebut Partnership for Battle Tech. Keterlibatan mendalam Palantir dalam infrastruktur militer Israel adalah bagian dari pola yang lebih luas dan mengkhawatirkan tentang teknologi yang memungkinkan peperangan. Hubungan itu meluas ke raksasa teknologi lainnya – Starlink milik SpaceX, yang dipimpin oleh Elon Musk. Memahami hubungan yang rumit ini sangat penting untuk memahami bagaimana konflik modern semakin didorong oleh teknologi canggih yang dikembangkan oleh perusahaan swasta.²³⁹

Pada akhir tahun 2021, CEO Microsoft, Satya Nadella, bertemu dengan komandan badan surveilans militer Israel, Unit 8200. Agenda pertemuan tersebut adalah memindahkan sejumlah besar materi intelijen rahasia ke cloud perusahaan AS tersebut. Kepala intelijen, Yossi Sarel, berhasil mendapatkan dukungan Nadella untuk sebuah rencana yang akan memberikan Unit 8200 akses ke area khusus dan terpisah di dalam platform cloud Azure milik Microsoft.²⁴⁰ Penggunaan sistem tersebut telah meningkat selama kampanye di Gaza dan telah menewaskan lebih dari 60.000 orang di wilayah tersebut, yang sebagian besar adalah warga sipil, termasuk lebih dari 18.000 anak-anak. Keterlibatan perusahaan dengan Unit 8200 didasarkan pada penguatan keamanan siber

²³⁷ Diyar Saraçoğlu, “From Productive Force to Destructive Force: Digital Colonialism in Palestine,” *bianet*, 7 Oktober 2025, <https://bianet.org/yazi/from-productive-force-to-destructive-force-digital-colonialism-in-palestine-312332>.

²³⁸ Saraçoğlu, “From Productive Force to Destructive Force.”

²³⁹ Business & Human Rights Resource Centre, “Palantir & Starlink Allegedly Complicit in War Crimes amid Israel’s War on Gaza,” 6 Juni 2024, <https://www.business-humanrights.org/en/latest-news/palantir-spacex-allegedly-licit-in-war-crimes-amid-israels-war-in-gaza/>.

²⁴⁰ Dengan kapasitas penyimpanan Azure yang hampir tak terbatas, Unit 8200 mulai membangun alat pengawasan massal baru yang ampuh: sebuah sistem yang luas dan invasif yang mengumpulkan dan menyimpan rekaman jutaan panggilan telepon seluler yang dilakukan setiap hari oleh warga Palestina di Gaza dan Tepi Barat. Harry Davies dan Yuval Abraham, “‘A Million Calls an Hour’: Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians,” *The Guardian*, 6 Agustus 2025, <https://www.theguardian.com/world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud>

dan melindungi Israel dari serangan siber negara dan teroris.²⁴¹ Kemudian menyusul investigasi yang diterbitkan oleh Guardian yang mengungkapkan bagaimana Azure digunakan untuk menyimpan dan memproses sejumlah besar komunikasi Palestina dalam program surveilans massal. Microsoft telah menghentikan akses militer Israel ke teknologi yang digunakannya untuk mengoperasikan sistem surveilans canggih yang mengumpulkan jutaan panggilan telepon warga sipil Palestina setiap hari di Gaza dan Tepi Barat, seperti yang diungkapkan Guardian Microsoft menyatakan pada 15 Agustus 2025, Unit 8200, badan mata-mata elit militer Israel telah melanggar ketentuan layanan perusahaan dengan menyimpan sejumlah besar data surveilans di platform cloud Azure.²⁴² Penghentian layanan Microsoft dilandasi prinsip perusahaan (1) tidak menyediakan teknologi untuk memfasilitasi surveilans massal terhadap warga sipil; dan (2) menghormati dan melindungi hak privasi pelanggan.²⁴³

Dalam kaitan itu, kompleks digital industrial militer dalam okupasi Israel atas Palestina, peran universitas signifikan sebagai bagian integral dari aparatus penindasan. Keterlibatan universitas semestinya dan tanggung jawab mereka dalam melanggengkan rezim apartheid dan dalam menghasilkan pengetahuan, teknologi, dan narasi yang fungsional bagi pendudukan. Departemen sains dan teknologi dari beberapa universitas berfungsi sebagai pusat penelitian dan pengembangan untuk kolaborasi antara militer Israel dan kontraktor senjata, termasuk Elbit Systems, IAI, IBM, dan Lockheed Martin, dan dengan demikian berkontribusi pada produksi piranti untuk surveilans, pengendalian massa, perang kota, pengenalan wajah, dan pembunuhan yang ditargetkan, piranti teknologi digital yang secara efektif diuji pada warga Palestina.²⁴⁴

²⁴¹ Davies dan Abraham, "A Million Calls an Hour': Israel Relying on Microsoft Cloud."

²⁴² Davies dan Abraham, "A Million Calls an Hour': Israel Relying on Microsoft Cloud."

²⁴³ Lihat komunikasi antara Amnesty International dengan Microsoft Israel/IOPT dalam Amnesty International, "Microsoft's Move to Block Israeli Military Unit's Access to Its Mass Surveillance Technology Is a Moment for Corporate Reckoning," 26 September 2025, <https://www.amnesty.org/en/latest/news/2025/09/microsoft-block-israel-military-unit-from-using-its-technology/>.

²⁴⁴ Massachusetts Institute of Technology (MIT) melakukan penelitian senjata dan surveilans yang didanai oleh Kementerian Pertahanan Israel (Israeli Ministry of Defense) membiayai penelitian MIT. Proyek-proyek Kementerian Pertahanan Israel, termasuk pengendalian kawanan drone, fitur khas serangan Israel di Gaza sejak Oktober 2023, algoritma pengejaran, dan surveilans bawah air. Dari tahun 2019 hingga 2024, MIT mengelola Lockheed Martin Seed Fund yang menghubungkan mahasiswa dengan tim di Israel. Dari tahun 2017 hingga 2025, Elbit Systems membayar keanggotaan MIT's Industrial Liaison Program yang memungkinkan akses ke penelitian dan talenta. Selain itu, Program Horizon Eropa Komisi Eropa secara aktif memfasilitasi kolaborasi dengan lembaga-lembaga Israel, termasuk mereka yang terlibat dalam apartheid dan genosida. Sejak 2014, Komisi Eropa telah memberikan lebih dari €2,12 miliar (\$2,4 miliar) kepada entitas Israel, termasuk Kementerian Pertahanan, sementara lembaga-lembaga akademis Eropa mendapat manfaat dari dan memperkuat keterlibatan ini. Technical University of Munich (TUM) menerima dana sebesar €198,5 juta (\$218 juta) dari program Horizon Komisi Eropa, termasuk €11,47 juta (\$12,6 juta) untuk 22 kolaborasi dengan mitra Israel, perusahaan militer dan teknologi. TUM dan Israel Aerospace Industries (IAI) menerima €792.795,75 (\$868.416) untuk bersama-sama mengembangkan pengisian bahan bakar hidrogen hijau, teknologi yang relevan dengan drone militer IAI yang digunakan di Gaza. TUM

Israel juga menggunakan media sosial sebagai piranti militer sebagai bagian dari kronik pendudukan militer Israel di wilayah Palestina dan bagaimana peran jejaring sosial sebagai agen dan mediator dalam hubungan tersebut. Persimpangan tersebut antara media sosial dan militerisme, antara praktik jejaring biasa (*ordinary networking practices*) dan kekerasan di masa perang (*wartime violence*), antara kesenangan dari tindakan digital yang umum (*pleasure of commonplace digital acts*) dan kebrutalan pendudukan militer Israel (*brutality of Israel's military occupation*).²⁴⁵ Adi Kuntsman dan Rebecca L. Stein menyebut fenomena ini sebagai militerisme digital (*digital militarism*) yang:

Menggambarkan proses yang meletakkan platform komunikasi digital dan praktik konsumen, selama dua dekade pertama abad ke-21, menjadi piranti militer di tangan aktor negara dan non-negara, baik di bidang operasi militer maupun dalam kerangka sipil.

bermitra dengan IBM Israel – yang mengelola Registrasi Penduduk Israel yang diskriminatif – dalam sistem cloud dan kecerdasan artifisial sebagai bagian dari pendanaan Horizon IBM Israel sebesar €7,02 juta (\$7,71 juta). TUM juga berkolaborasi dalam proyek senilai €10,76 juta (\$11,71 juta) yang disebut seamless urban mobility (mobilitas perkotaan tanpa batas) yang mencakup Kota Yerusalem, sebuah kota yang memperkuat aneksasi melalui transportasi perkotaan. Tidak mungkin untuk memisahkan keahlian yang disumbangkan oleh mitra Israel ke dalam kemitraan ini dari keahlian yang diperoleh dan digunakan dalam pelanggaran yang terkait dengan mereka. Lebih jauh, banyak universitas telah mempertahankan hubungan dengan Israel meskipun terjadi eskalasi pasca-Oktober 2023. Salah satu dari banyak contoh di Inggris, Universitas Edinburgh memegang hampir £25,5 juta (\$31,72 juta) (2,5 persen dari dana abadi) di empat raksasa teknologi – Alphabet, Amazon, Microsoft, dan IBM – yang menjadi pusat aparat surveilans Israel dan penghancuran Gaza yang sedang berlangsung. Dengan investasi langsung dan terindeks, universitas ini termasuk di antara lembaga-lembaga di Inggris yang paling terjerat secara finansial. Universitas ini juga bermitra dengan perusahaan yang membantu operasi militer Israel, termasuk Leonardo S.p.A. dan Universitas Ben Gurion melalui Laboratorium Kecerdasan Artifisial dan Ilmu Data, berbagi penelitian yang secara langsung menghubungkannya dengan serangan terhadap warga Palestina. Lihat, Albanese, *From Economy of Occupation to Economy of Genocide*.

²⁴⁵ Selama masa penantian serangan, tentara Israel mengunggah serangkaian foto diri ke akun Instagram pribadi mereka. Katalog standar potret diri menggunakan ponsel pintar, termasuk foto-foto kasual militer muda berseragam yang tersenyum ke kamera sesuai dengan investasi Instagram dalam keindahan hal-hal biasa, menampilkan momen sehari-hari kehidupan militer berseragam, seperti naik bus, berpose untuk potret diri di lift, memeluk seorang teman, semuanya dibingkai oleh temporalitas penantian yang panjang, menunggu untuk dikerahkan. Dengan bantuan filter retro, dan estetika, foto-foto seluler ini menghasilkan arsip visual yang indah dan sangat bersih tentang kehidupan militer. Dengan demikian, mereka menawarkan sentuhan digital pada sejarah panjang sentimen nasionalis Israel dan ikonografi terkait, di mana perang secara bersamaan dipuja dan diestetisasi sementara dipisahkan dari kekerasan yang diakibatkannya. Militer Israel memobilisasi melalui genre selfie, ikonografi untuk melayani kebutuhan pencitraan diri, dengan perang dikonfigurasi sebagai meme dan digunakan sebagai alat mikro-selebriti. Foto-foto militerisme tetapi bukan pertempuran, tubuh yang diperindah bebas dari kotoran atau darah, yang cukup jauh dari pembantaian operasi militer yang terjadi bersamaan. Rangkaian tagar yang menyertainya mengisyaratkan kekerasan yang telah dibersihkan oleh bidang visual. Jika dibaca bersama, swafoto dan tagar yang menyertainya menghasilkan persimpangan yang meresahkan antara patriotisme dan keintiman, mematikan dan main-main, tentara dan algoritma. Lihat, Adi Kuntsman dan Rebecca L. Stein, *Digital Militarism: Israel's Occupation in the Social Media Age* (Redwood City: Stanford University Press, 2015).

Apabila menelisik pemaknaan militerisme digital, maka okupasi militer pada ranah digital juga merupakan manifestasi piranti teknologi dwiguna dalam konteks militerisasi teknologi.

Secara umum, menurut Adi Kuntsman dan Rebecca L. Stein digital dari militerisme digital (*digital of digital militarism*) adalah domain yang sangat beragam dari teknologi baru dan kemampuan teknologi, termasuk persenjataan berteknologi tinggi dan perang siber dan Israel dengan bangga merasa unggul dalam penguasaan militerisasi teknologi. Selama okupasi Israel peran media sosial dan teknologi seluler mendukung dengan cara negara memobilisasi media sosial dan teknologi seluler dan publik yang terhubung sebagai piranti, situs, dan bahasa keterlibatan militeristik. Oleh karena itu, istilah militerisme digital merujuk pada perluasan budaya militer ke domain media sosial yang sering dianggap di luar jangkauan kekerasan negara, dan pada dampak militerisasi terhadap jejaring sosial sehari-hari di Israel. Dalam konteks okupasi Israel kedua istilah ini saling membentuk satu sama lain, yaitu, istilah penggunaan media sosial yang berkembang berdampak pada bidang militerisme Israel, sama seperti pergeseran dalam militerisasi Israel mengubah bidang media sosial.²⁴⁶

Militerisme digital sebagai strategi hubungan masyarakat (*public relation*) secara sistematis untuk memperlihatkan berbagai cara yang beragam dan seringkali biasa terjadi dalam mempertahankan dan melestarikan rezim militer Israel dan budaya militerisme yang meluas. Militerisasi media sosial sama sekali bukan hal yang unik dalam konteks Israel. Sebaliknya, seperti yang sekarang sudah menjadi kebenaran umum, media sosial telah diintegrasikan ke dalam operasi militer dalam berbagai konteks di seluruh dunia, dengan platform seperti Twitter, Instagram, dan YouTube. Piranti media sosial ini digunakan sebagai strategi hubungan masyarakat masa perang, sebagai piranti surveilans dan kontra-pemberontakan, dan sebagai arsip kekerasan pelaku. Di era media sosial, peperangan kontemporer dan konflik bersenjata semakin mencakup platform komunikasi digital sebagai suatu proses yang telah memperluas teater operasi militer dan upaya mengubah pemahaman pengguna tentang fungsi politik dan tujuan politik teknologi digital.²⁴⁷

Ketika Israel meluncurkan operasi Pillar of Defense pada November 2012, Israel menggunakan platform media sosial untuk pertama kalinya sebagai instrumen perang. Perluasan kampanye militer Israel ke media sosial bukan hanya oleh pengguna sipil di berbagai lokasi, baik di Israel, Palestina, dan arena internasional, tetapi juga oleh unit media sosial resmi militer Israel. Militer memilih akun Twitter khusus mereka untuk

²⁴⁶ Kuntsman dan Stein, *Digital Militarism*.

²⁴⁷ Kuntsman dan Stein, *Digital Militarism*.

mengumumkan dimulainya operasi, sementara mereka juga menyiapkan konten di platform lain, seperti YouTube, Flickr, Pinterest, dan Facebook.²⁴⁸

Gambaran di atas memperlihatkan bagaimana Israel mengembangkan industri senjata kelas dunia dengan cara mengujikannya pada warga Palestina yang diduduki, kemudian dipasarkan sebagai "teruji di medan perang." Memanfaatkan merek IDF (*Israeli Defense Forces*) telah berhasil menjadikan perusahaan keamanan Israel sebagai beberapa perusahaan paling sukses di dunia. Laboratorium Palestina (*Palestine laboratory* menjadi salah satu nilai jual persenjataan Israel. Bahkan laboratorium Palestina telah menjadi kebijakan negara hampir selama pendudukan Israel atas wilayah Palestina.²⁴⁹ Perangkat *spyware* Pegasus yang diproduksi NGO²⁵⁰ dan Cellebrite menyebabkan kerusakan di seluruh dunia terlahir dari sejarah militerisme Zionis untuk mengembangkan industri pertahanan dan kemudian menjual serta mempromosikannya ke pasar global.²⁵¹ Ron Deibert berpendapat tantangan utama untuk menentang industri surveilans siber bagaimana mengatasi fakta bahwa dunia saat ini dijalankan oleh kelas gangster transnasional (*the world today is run by a transnational class of gangsters*). Oleh karena itu, tanpa perubahan mendasar pada insentif finansial yang melekat pada perusahaan seperti NSO, masa depan kondisi manusia suram. Surveilans data pribadi dan kontrol negara otoriter menjadi Peluang bisnis yang tampaknya tak terbatas dan menguntungkan yang merusak akuntabilitas publik dan memfasilitasi pemerintahan despotik.²⁵²

²⁴⁸ Pasca 2012 terjadi pergeseran substansial dalam ranah militerisme digital Israel. Pada tahun-tahun sebelumnya, militer terutama menggunakan internet untuk kontra-pemberontakan atau sebagai media siaran untuk pesan-pesan didaktik. Pada 2012, militer Israel menggunakan media sosial dengan cara yang sangat berbeda. Selama invasi tersebut, platform seperti Facebook dan Twitter menjadi piranti perang tersendiri, yang diubah menjadi apa yang disebut "teknologi peringatan" dan deklarasi perang. Kontras dengan kampanye 2008–2009, menurut banyak pakar, sangat mencolok. Dari berbagai sudut pandang media, militer mendapat ucapan selamat atas peningkatan efektivitas, skala, dan ketepatan waktu keterlibatan media sosialnya. Di Israel, seperti di banyak konteks geopolitik lainnya, militerisasi internet dimulai dalam bentuk peretasan. Komunitas Online Israel pertama kali demiliterisasi secara besar-besaran selama invasi militer tahun 2008–2009 di Jalur Gaza, yang diberi kode nama Operasi Cast Lead. Invasi Gaza tahun 2008–2009 merupakan tonggak sejarah: penggunaan media sosial resmi pertama oleh militer Israel. Kebutuhan strategi hubungan masyarakat melalui media sosial muncul dari pelajaran perang Lebanon kedua dengan Hizbullah pada 2006 ketika militer Israel dikatakan telah kalah dalam pertempuran informasi karena berbagai kesalahan teknologi. Lihat, Kuntsman dan Stein, *Digital Militarism*.

²⁴⁹ Loewenstein, *The Palestine Laboratory*.

²⁵⁰ Kekuatan NSO dan negara Israel hampir tak terbendung, bahkan menjerat Apple yang terpaksa mengeluarkan pembaruan perangkat lunak darurat pada 2021 untuk 1,65 miliar penggunanya setelah Citizen Lab menemukan kerentanan dalam sistem operasinya yang telah dieksploitasi oleh NSO. Apple mengeluarkan siaran pers dan secara langsung menyatakan keterlibatan Israel. NSO Group menciptakan teknologi surveilans canggih yang disponsori negara yang memungkinkan perangkat lunak mata-mata (*spyware*) yang sangat tertarget untuk mengawasi korbannya. Lihat Loewenstein, *The Palestine Laboratory*.

²⁵¹ Loewenstein, *The Palestine Laboratory*.

²⁵² Loewenstein, *The Palestine Laboratory*.

Pemerintah Indonesia menentang tindakan Israel atas Palestina, dan bahkan sampai saat ini, Pemerintah Indonesia tidak memiliki hubungan diplomatik dengan Israel. Namun pada saat bersamaan Pemerintah Indonesia tetap membeli piranti *spyware* yang dikembangkan dan diuji pada warga Palestina. Piranti *spyware* asal Israel penting untuk diletakkan dalam konteks Palestina telah menjadi laboratorium yang sempurna (*Palestine has become the perfect laboratory*) bagi kompleks teknologi-militer (*Israeli military-techno complex*), meliputi surveilans, penghancuran rumah, penahanan tanpa batas waktu, dan kebrutalan hingga piranti berteknologi tinggi yang dihasilkan perusahaan-perusahaan rintisan (*start-up nation*). Israel telah menjadi pemimpin global dalam teknologi *spyware* dan perangkat keras pertahanan yang memicu konflik paling brutal di dunia. Seiring dengan tumbuhnya etno-nasionalisme di abad ke-21, Israel telah membangun model pamungkasnya. teknologi pertahanan dan surveilans baru yang akan dipamerkan kepada investor dan klien internasional, termasuk Indonesia.²⁵³

Israel dan Indonesia tidak memiliki hubungan diplomatik formal, meskipun terjalin kontak perdagangan, pariwisata, dan keamanan secara diam-diam. Pada tahun 2008, nilai perdagangan antara Indonesia dan Israel mencapai \$900 juta dengan \$300 juta berasal dari batubara. Perdagangan antara Jakarta dan Tel Aviv dilaporkan mencapai \$550 juta pada 2021, 84 persen di antaranya adalah ekspor Indonesia. Sementara Indonesia terutama mengeksport komoditas, ekspor Israel terutama berupa produk teknologi tinggi dan piranti lunak siber.²⁵⁴

Israel adalah rumah bagi lebih banyak perusahaan *spyware* daripada negara lain mana pun di dunia, termasuk NICE, Verint, NSO Group, Black Cube, Candiru, Cyrox, Cellebrite, dan Intellexa. Teknologi *spyware* ini dirancang dan diuji sebagai bagian dari pendudukan Israel dan rezim apartheid di Palestina. Setelah teknologi tersebut berhasil diuji, perusahaan *spyware* Israel diizinkan oleh Kementerian Pertahanan Israel untuk menjual teknologi tersebut demi keuntungan.²⁵⁵ Dari 75 pemerintah yang telah membeli *spyware* dan teknologi forensik digital di seluruh dunia, 56 membelinya dari perusahaan yang berbasis di atau terhubung dengan Israel, seperti NSO Group, Cellebrite, Cyrox, dan Candiru. Semua kesepakatan ini dipantau dan disetujui oleh Kementerian Pertahanan Israel. Bagi Israel, *spyware* bukan hanya industri yang sangat menguntungkan, tetapi juga senjata strategis untuk mendapatkan dukungan diplomatik. Selain merevolusi dunia spionase, permintaan besar akan piranti ini membentuk kembali geopolitik, dengan nyawa warga Palestina berada di ujung tombak permainan *spyware* global yang jahat.²⁵⁶ Industri piranti *spyware* negara telah diuntungkan dari perputaran

²⁵³ Loewenstein, *The Palestine Laboratory*.

²⁵⁴ DIMSE, "Indonesia," <https://dimse.info/indonesia/>.

²⁵⁵ War on Want, "Israeli Spyware Is Threatening Our Rights and Freedoms," <https://waronwant.org/resources/israeli-spyware-threatening-our-rights-and-freedoms>.

²⁵⁶ Menurut investigasi New York Times, kesepakatan NSO telah memainkan peran sentral dalam mengamankan dukungan dari negara-negara Arab, termasuk dalam negosiasi Perjanjian Abraham,

petugas intelijen, khususnya Unit 8200. Setelah menghabiskan hari-hari mereka memantau setiap aspek kehidupan Palestina, pengalaman tersebut dibawa ke sektor swasta untuk merancang dan mengembangkan piranti surveilans paling canggih dan diekspor ke seluruh dunia, baik ke negara demokrasi maupun kediktatoran. Warga Palestina yang diduduki menjadi kelinci percobaan ketika senjata pendudukan Israel dikembangkan dan diuji.²⁵⁷ Beberapa Perusahaan teknologi digital asal Israel yang diidentifikasi dipergunakan di Indonesia dapat diuraikan di bawah ini:

1. Cellebrite

Cellebrite telah menjual pirantinya ke Indonesia, padahal dan menggunakannya untuk menargetkan lawan politik dan aktivis, termasuk di Papua Barat dan menysasar kelompok minoritas seksual. Selain itu, Indonesia menggunakan teknologi penyadapan komunikasi dari perusahaan Israel Verint Systems dan menggunakan piranti tersebut untuk mengintersepsi komunikasi komunitas minoritas seksual.²⁵⁸ Sementara selama serangan genosida di Gaza, Israel menggunakan piranto Cellebrite untuk mengumpulkan data dari ponsel ribuan warga Palestina yang ditangkap dan diculik dari Gaza. Meskipun media Israel mengklaim bahwa semua individu tersebut adalah anggota kelompok militan, militer Israel kemudian mengakui bahwa sebagian besar adalah warga sipil. Cellebrite juga menerima dana dari unit inovasi Pentagon untuk mengembangkan produk guna memetakan terowongan bawah tanah di Jalur Gaza.²⁵⁹ Pada tahun 2019 Cellebrite berpartisipasi dalam KTT Keamanan Tahunan Indonesia (Annual Indonesia Security Summit) di Jakarta, Indonesia. Perusahaan terkemuka Indonesia di bidang forensik digital, Bouna Solusi Informatika, penyedia resmi piranti *Universal Forensic Extraction Device (UFED)* di Indonesia. Pada 2019, CNN melaporkan bahwa Kepolisian Indonesia menggunakan teknologi Cellebrite untuk mengekstrak data dari orang-orang yang dituduh melakukan ujaran kebencian. Teknologi ini juga dilaporkan digunakan untuk mengekstrak data aktivis Indonesia. Pada 2020, Haaretz melaporkan bahwa Indonesia menggunakan teknologi Cellebrite untuk membungkam

perjanjian diplomatik tahun 2020 yang menormalisasi hubungan antara Israel dan negara-negara Arab seperti Bahrain dan Uni Emirat Arab. Akibatnya, perusahaan seperti NSO Group dapat dilihat sebagai lengan tidak resmi negara Israel, yang memperkuat hubungan militer dan diplomatik negara tersebut. Lihat, New Internationalist, "How Palestine Became Israel's Spyware Test-Bed," <https://newint.org/features/2023/10/02/spy-games>.

²⁵⁷ New Internationalist, "How Palestine Became Israel's Spyware Test-Bed."

²⁵⁸ New Internationalist, "How Palestine Became Israel's Spyware Test-Bed.". Lihat juga Amnesty Internasional, *A Web Of Surveillance*.

²⁵⁹ American Friends Service Committee, "Companies Profiting from the Gaza Genocide," <https://afsc.org/gaza-genocide-companies>.

perbedaan pendapat politik dan untuk menegakkan hukum kesusilaan yang kontroversial.²⁶⁰

2. Saito Tech, juga dikenal sebagai Candiru

Saito Tech vendor surveilans siber asal Israel yang menawarkan sistem infiltrasi siber, yang dipasarkan dengan nama Cyrus. Teknologi ini dirancang untuk menginfiltrasi komputer PC, jaringan, dan piranti seluler, dengan menggunakan eksploitasi dan operasi penyebaran. Menurut proposal komersial Candiru yang bocor dari tahun 2020 beberapa kemampuan Candiru membahayakan PC Windows serta perangkat seluler Android dan iOS.²⁶¹ Vendor piranti Israel yang terdaftar sebagai Saito Tech Ltd. Candiru adalah perusahaan Israel, sehingga setiap penjualan merupakan ekspor pertahanan yang membutuhkan lisensi dari Kementerian Pertahanan Israel. Perusahaan ini dimiliki secara pribadi, tidak menerbitkan laporan keuangan, dan telah mengubah nama terdaftarnya empat kali. Perusahaan ini masih dapat dipindahkan, karena bergantung pada tiga hal yang tidak dapat dikendalikannya: (1) lisensi ekspor Israel; (2) dana Amerika yang membeli asetnya pada 2025, dan (3) pemerintah yang bersedia menandatangani perjanjian. Microsoft menghitung lebih dari 100 korban, termasuk politisi, jurnalis, akademisi, pekerja kedutaan, aktivis HAM, dan pembangkang politik, dan menempatkan sekitar setengah dari mereka di Palestina. Avast melaporkan pada Juli 2022 bahwa Candiru mengeksploitasi celah keamanan di Google Chrome terhadap pengguna di Lebanon, Turki, Yaman, dan Palestina, Kemudian, Kementerian Pertahanan Israel mengurangi daftar negara-negara tempat perusahaan Israel dapat mengekspor perangkat siber ofensif dari 102 menjadi 37, dengan menghapus Arab Saudi dan Uni Emirat Arab. Setiap penjualan Candiru dilisensikan berdasarkan daftar tersebut, sehingga negara Israel, yang memutuskan siapa yang boleh membeli bukan perusahaan.²⁶² Amnesty International menemukan pengiriman piranti keras, yang dikaitkan Amnesty International dengan sistem Candiru, kepada Kepolisian Nasional Indonesia sebagai pengguna akhir melalui Heha PTE Ltd (Heha) yang berbasis di Singapura.²⁶³

²⁶⁰ DIMSE, "Indonesia."

²⁶¹ Amnesty Internasional, *A Web of Surveillance*.

²⁶² Stop Palestinian Genocide memasukkan Saito Tech Ltd. (Candiru) sebagai target prioritas kampanye karena perusahaan tersebut dinilai memiliki tingkat bahaya yang tinggi dalam konteks pendudukan Israel di Palestina dan cukup rentan terhadap tekanan kampanye. Lihat, Stop Palestinian Genocide, "Candiru (Saito Tech Ltd)," <https://palestiniangenocide.org/boycott/companies/candiru/>.

²⁶³ Meskipun pengiriman dari Heha kepada Kepolisian Nasional Indonesia tidak menyertakan nama produk atau perusahaan yang dapat diidentifikasi, Amnesty International melakukan pengecekan silang dan menemukan terdapat korelasi signifikan antara deskripsi dan waktu pengiriman yang

3. NSO Group

NSO Group adalah perusahaan yang berbasis di Israel yang mengembangkan dan menjual platform spyware Pegasus yang dirancang untuk secara diam-diam membahayakan perangkat seluler seperti iPhone dan perangkat Android, serta Blackberry. Kelompok investigasi IndonesiaLeaks dan mitra medianya, termasuk Tempo, menerbitkan investigasi pada Juni 2023 yang mengidentifikasi Indonesia sebagai pelanggan potensial piranti spyware Pegasus milik NSO Group dan telah digunakan untuk menargetkan anggota masyarakat sipil secara ilegal di seluruh dunia. Temuan IndonesiaLeaks didasarkan pada analisis catatan impor dan pernyataan dari beberapa sumber anonim yang menunjukkan Pegasus dijual ke, dan digunakan di, Indonesia. Selain itu, IndonesiaLeaks juga melaporkan Kepolisian Negara Republik Indonesia dan Badan Intelijen Negara (BIN) telah memperoleh akses ke Pegasus.²⁶⁴ Setiap penjualan membutuhkan izin ekspor dari Kementerian Pertahanan Israel, sehingga negara Israel yang memutuskan siapa yang mendapatkannya. Citizen Lab, sebuah kelompok riset di Universitas Toronto, dan Security Lab Amnesty International secara independen mengkonfirmasi keberadaan Pegasus pada perangkat enam pembela hak asasi manusia Palestina pada 8 November 2021. Israel telah menetapkan enam organisasi masyarakat sipil Palestina sebagai organisasi teroris beberapa minggu sebelumnya. Front Line Defenders berpendapat bahwa penetapan tersebut sebagian merupakan upaya untuk melegitimasi surveilans yang sudah dilakukan terhadap staf mereka. Seorang penyelidik PBB, Pelapor Khusus untuk wilayah Palestina yang diduduki, mencatat pada 30 Juni 2025 bahwa Pegasus telah digunakan terhadap aktivis Palestina. Meskipun sudah berganti kepemilikan kepada investor asal Amerika Serikat NSO Group mengatakan investasi tersebut tidak berarti perusahaan tersebut keluar dari kendali pengaturan atau operasional Israel. Kantor pusat dan operasi intinya tetap berada di Israel, dan masih sepenuhnya diawasi dan diatur oleh Kementerian Pertahanan Israel. Setiap penjualan membutuhkan lisensi dari Badan Pengendalian Ekspor Pertahanan (*Defense Export Control Agency*), badan ekspor kementerian tersebut. Laporan PBB yang sama menemukan bahwa ekspor semacam itu memungkinkan diplomasi spyware sembari memperkuat impunitas negara. Pembelaan NSO adalah bahwa pelanggannya, bukan NSO, yang memilih siapa yang menjadi target²⁶⁵

menunjukkan Candiru sebagai pemasok sistem surveilans siber ini. Lihat, Amnesty Internasional, *A Web of Surveillance*.

²⁶⁴ Amnesty Internasional, *A Web of Surveillance*.

²⁶⁵ Stop Palestinian Genocide memasukkan Saito Tech Ltd. (Candiru) sebagai target prioritas kampanye karena perusahaan tersebut dinilai memiliki tingkat bahaya yang tinggi dalam konteks pendudukan Israel di Palestina dan cukup rentan terhadap tekanan kampanye. Lihat Stop Palestinian

4. Wintego Systems Ltd (Wintego)

Wintego merupakan perusahaan surveilans siber Israel yang memasarkan perangkat spyware untuk ponsel pintar dan berbagai teknologi intersepsi jaringan taktis dengan merek WINT. Amnesty International mengidentifikasi infrastruktur jaringan yang terkait dengan spyware Helios milik Wintego, serta domain berbahaya yang digunakan di Indonesia dan negara lain. Amnesty International mengidentifikasi reseller Wintego berkedudukan di Singapura: Ataka Enterprises PTE Ltd (Ataka). Berdasarkan data pengiriman dari basis data komersial dan informasi yang diposting di situs web dan postingan blog, Amnesty International telah menemukan informasi yang menunjukkan bahwa produk pengawasan siber Wintego dijual kepada Kepolisian Negara Republik Indonesia melalui dua perusahaan yang berbasis di Singapura, Ataka dan ESW System.²⁶⁶

5. Cognyte/Verint

Pada 2018, Haaretz mengungkapkan penggunaan produk Verint untuk surveilans yang tidak semestinya terhadap aktivis minoritas seksual dan kelompok minoritas agama. Pada 2021, Verint memisahkan divisi intelijen siber dan pertahanannya menjadi perusahaan independen bernama Cognyte. Perusahaan baru tersebut melanjutkan aktivitasnya di Indonesia. Pada Februari 2022, Intelligence Online melaporkan bahwa perusahaan asal Israel, Cognyte, mendapatkan kontrak dari badan intelijen Indonesia;²⁶⁷

6. Corsight AI

Pada tahun 2021, Corsight AI mengumumkan akan memperluas bisnisnya di wilayah-wilayah utama di Asia, termasuk Indonesia. Pada Mei 2021, Corsight AI bermitra dengan Netpoleon, Value-Added Distributor (VAD) produk Jaringan dan Keamanan Siber yang berkantor pusat di Singapura, untuk membuat teknologi pengenalan wajah lebih mudah diakses di seluruh wilayah Asia, termasuk Indonesia;²⁶⁸

7. BriefCam

Menurut dokumen resmi Perusahaan produk BriefCam digunakan oleh Kepolisian Indonesia.²⁶⁹

Genocide, "NSO Group," *Stop the Palestinian Genocide*,
<https://palestiniangenocide.org/boycott/companies/nsol/>.

²⁶⁶ Amnesty International, *A Web of Surveillance*.

²⁶⁷ DIMSE, "Indonesia."

²⁶⁸ DIMSE, "Indonesia."

²⁶⁹ DIMSE, "Indonesia."

Penggunaan spyware oleh Pemerintah Indonesia yang telah diujicobakan kepada warga Palestina dan juga digunakan sebagai bagian dari surveilans negara merupakan manifestasi dari praktik mis-apropriasi HAM (*mis-appropriation of human rights*). Dalam acara KTT untuk Penyelesaian Damai atas Masalah Palestina dan Implementasi Solusi Dua Negara, salah satu rangkaian acara sidang umum PBB, Prabowo menyampaikan pidato menyerukan kemerdekaan Palestina.²⁷⁰

"Kita harus mengakui Palestina sekarang. Kita harus menghentikan bencana kemanusiaan di Gaza... Mengakhiri perang harus menjadi prioritas utama kita. Kita harus mengatasi kebencian, ketakutan, dan kecurigaan. Kita harus mencapai perdamaian yang dibutuhkan umat manusia. Dengan berat hati, kami mengenang tragedi yang tak tertahankan dan berkelanjutan di Gaza. Ribuan nyawa tak berdosa, banyak di antaranya perempuan dan anak-anak, telah terbunuh. Kelaparan mengancam. Bencana kemanusiaan sedang terjadi di depan mata kita."

Meskipun Presiden Prabowo Subianto mengutuk serangan Israel atas Gaza yang terus berlanjut, namun demikian, Presiden belum memperhitungkan senjata Israel, Pegasus yang masih mungkin beroperasi di dalam negeri. Pegasus dan piranti spyware lainnya merupakan instrumentasi pendudukan Israel, kemudian ditransformasi menjadi instrumen perdagangan untuk dipasarkan sebagai piranti lunak kontraterorisme dan melalui jaringan perantara dan perusahaan lokal, Pegasus dan produk spyware asal Israel ini diam-diam mensurveilans warga negara yang kritis. Pada titik ini, Presiden Prabowo Subianto menunjukkan politik misapropriasi HAM karena nampak menggunakan wacana HAM untuk mengecualikan atau menindas kelompok dan individu tertentu sambil memperkuat otoritasnya.²⁷¹

Presiden Prabowo Subianto berdiri dalam solidaritas dengan Gaza, namun pada saat bersamaan tidak membongkar jejak digital Israel di dalam negeri. Pegasus bukan hanya produk; itu adalah bagian dari ekonomi pendudukan Israel. Pegasus telah mengalami penyempurnaan karena telah diujicobakan kepada warga Palestina, kemudian dimonetisasi secara global. Pegasus membawa logika pendudukan ke mana pun Pegasus dipasarkan dan diperdagangkan bahwa perbedaan pendapat adalah ancaman, minoritas adalah tersangka, kritikus adalah musuh.²⁷² Lebih jauh, nampak jelas kecenderungan Presiden Prabowo Subianto memaknai HAM dilandasi imajinasinya

²⁷⁰ Deutsche Welle, "Poin-poin Pernyataan Prabowo soal Palestina di KTT PBB," <https://www.dw.com/id/poin-poin-pernyataan-prabowo-soal-palestina-di-ktt-pbb/a-74102466>.

²⁷¹ Gráinne de Búrca dan Katharine G. Young, "The (Mis)appropriation of Human Rights," *Open Global Rights*, <https://www.openglobalrights.org/misappropriation-human-rights/>.

²⁷² Muhammad Zulfikar Rakhmat, "Indonesia Cannot Condemn Gaza Genocide While Still Silent on Its Use of Israeli Spyware," *Middle East Monitor*, 30 September 2025, <https://www.middleeastmonitor.com/20250930-indonesia-cannot-condemn-gaza-genocide-while-still-silent-on-its-use-of-israeli-spyware/>.

sendiri, seperti kata antek asing, londo ireng, pelaku makar dan teroris yang ditujukan kepada individu atau kolektif yang mengkritik pemerintah.

Menurut analisis Tempo sebutan “antek asing” kerap ditujukan kepada pengkritik pemerintah. Frekuensi kata asing semakin sering seiring berbagai demonstrasi yang menentang berbagai kebijakan Presiden Prabowo Subianto. Bahkan saat berpidato dalam hari ulang tahun Partai Gerindra ke-17 dan peringatan Hari Lahir Pancasila, Presiden Prabowo Subianto secara eksplisit menuding ada lembaga swadaya masyarakat dan media yang dibayar asing untuk mengacaukan Indonesia.²⁷³

Namun pada saat yang sama Presiden Prabowo Subianto juga menggunakan wacana HAM dan demokrasi yang dibangun dengan narasinya sendiri. Ambil contoh ketika berpidato dalam pelantikannya sebagai Presiden menyatakan menginginkan demokrasi santun khas Indonesia, minim permusuhan dan mengoreksi tanpa caci maki. Pidato ini menyiratkan kehendak Presiden Prabowo Subianto demokrasi santun dapat diterjemahkan sebagai pelarangan berbicara dan protes demi menjaga ketertiban umum. Pada akhirnya, kesantunan dalam berdemokrasi hanya diukur dari kacamata penguasa.²⁷⁴

Presiden Prabowo Subianto kemudian menyatakan penerapan HAM dan demokrasi ala Barat dinilainya bersifat hipokrit. Presiden Prabowo Subianto kemudian menyinggung negara-negara Barat yang mengajarkan demokrasi tetapi tetap menjajah Indonesia selama ratusan tahun. Ia juga menyebut negara Barat sering mengajarkan HAM, tetapi dalam praktiknya ikut melanggar HAM.²⁷⁵

Perspektif Presiden Prabowo dapat dimaknai sebagai upaya untuk memeriksa kembali kesesuaian HAM dan mengidentifikasi HAM mana asal Barat dan HAM mana asli Indonesia. Dengan demikian, upaya untuk memeriksa kembali kesesuaian HAM akan diikuti penolakan kerangka kerja HAM internasional yang telah terkanonisasi dalam sistem HAM PBB. Perspektif ini nampaknya merangkul wacana HAM dan memposisikan diri sebagai penafsir otoritatif memaknai HAM dengan semangat ke-Indonesia-an. Namun apabila ditelisik lebih jauh, alih-alih memperbarui komitmen Presiden terhadap HAM, penyematan HAM ala Barat tersebut justru upaya apropriasi HAM dengan mengubah kanon HAM dari dalam dengan meninggikan beberapa HAM yang diklaim sebagai identitas Indonesia. Konsekuensi lebih lanjut upaya ini justru akan mempersempit HAM sesuai dengan pandangan sosial-politik konservatif untuk memilah

²⁷³ BBC News Indonesia, “Aparat membungkam jurnalis dan aktivis dengan narasi antek asing, sebut laporan,” 20 Mei 2026, <https://www.bbc.com/indonesia/articles/cj4pqkw785lo>.

²⁷⁴ Tempo, “Demokrasi Santun Prabowo Subianto,” 23 Oktober 2024, <https://www.tempo.co/kolom/demokrasi-santun-prabowo-subianto-1096274>.

²⁷⁵ Tempo, “Natalius Pigai Respons Kritik Prabowo terhadap HAM Barat Hipokrit,” 9 Desember 2025, <https://www.tempo.co/hukum/natalius-pigai-respons-kritik-prabowo-terhadap-ham-barat-hipokrit-2097231>.

dan memilih dari mana HAM berasal, siapa yang paling dilindungi oleh hak-hak tersebut, dan hak mana yang lebih penting daripada yang lain.²⁷⁶

Sementara itu, Presiden Prabowo Subianto menghendaki Indonesia menjadi anggota Board of Peace yang diinisiasi oleh Presiden Amerika Serikat, Donald Trump.²⁷⁷ Kemudian Dewan Keamanan PBB pada 17 November 2025, mengadopsi Resolusi 2803, yang dikenal sebagai Board of Peace. Resolusi tersebut menyerukan kepada semua pihak untuk menerapkan rencana komprehensif Donald Trump dan menjaga gencatan senjata dengan itikad baik dan tanpa penundaan. Paragraf 2, resolusi tersebut menggambarkan Board of Peace sebagai pemerintahan transisi dengan kepribadian hukum internasional yang akan memerintah Jalur Gaza hingga Otoritas Palestina menyelesaikan reformasinya sesuai jadwal. Lebih lanjut dinyatakan bahwa penentuan nasib sendiri dan kedaulatan negara Palestina dapat dicapai ketika program reformasi Otoritas Palestina selesai dan pembangunan kembali Jalur Gaza berjalan lancar.²⁷⁸

Hal ini bertentangan dengan prinsip hukum internasional bahwa hak penentuan nasib sendiri rakyat Palestina adalah hak yang tidak dapat dicabut yang diabadikan dalam hukum internasional dan tidak dapat dikenakan prasyarat, seperti reformasi Otoritas Palestina dan kemajuan rencana pembangunan kembali Gaza.²⁷⁹ Francesca Albanese mendukung posisi ini, dengan menyatakan bahwa:

²⁷⁶Jayne Huckerby, Sarah Knuckey, Appropriation and the rewriting of rights, *International Journal of Constitutional Law*, Volume 21, Issue 1, January 2023

²⁷⁷ Niat Presiden Amerika Serikat Trump membentuk Dewan Perdamaian dibuktikan dalam Perintah Eksekutif (Executive Order) 14375 yang menetapkan dewan tersebut sebagai organisasi internasional publik. Demikian pula, piagam dewan tersebut menetapkan bahwa dewan dan entitas turunannya akan memiliki kepribadian hukum internasional dan akan memastikan penyediaan hak istimewa dan kekebalan yang diperlukan untuk menjalankan fungsi. Sebelumnya Menteri Luar Negeri Amerika Serikat Marco Rubio mengkonfirmasi kepada anggota Senat bahwa dewan tersebut akan memiliki status hukum yang sama dengan PBB. Namun kemudian, Marco Rubio selama kesaksiannya di hadapan Komite Hubungan Luar Negeri Senat menyatakan bahwa pemerintahan Donald Trump telah memutuskan untuk mengubah Dewan Perdamaian dari organisasi internasional publik yang terdiri dari negara-negara anggota menjadi organisasi nonpemerintah internasional (INGO). Lihat Zaha Hassan, "Board Up Donald Trump's Failed Board of Peace," *Carnegie Endowment for International Peace*, 17 Juni 2026, <https://carnegieendowment.org/middle-east/diwan/2026/06/board-up-trumps-failed-board-of-peace>.

²⁷⁸ Mohammad Yousef, "Why the Recent UNSC Resolution 2803 'Board of Peace' Violates the UN Charter," *Middle East Monitor*, 21 November 2025, <https://www.middleeastmonitor.com/20251121-why-the-recent-uns-rc-resolution-2803-board-of-peace-violates-the-un-charter/>.

²⁷⁹ Pendapat penasihat Mahkamah Internasional baru-baru ini pada tahun 2024, yang semuanya menyimpulkan bahwa pendudukan Israel di Wilayah Pendudukan Palestina (OPT), termasuk Jalur Gaza, adalah pendudukan ilegal yang bersifat agresif, menyerukan Israel untuk menarik diri dari semua wilayah yang didudukinya pada tahun 1967. Sementara itu, Resolusi 2803 tidak menyebutkan pendudukan Israel atau menyerukan penarikan penuhnya. Namun, resolusi tersebut menyerukan negara-negara anggota International Stabilisation Forces (ISF) untuk bekerja dan bekerja sama dengan Israel. Israel, sebagai kekuatan pendudukan, tidak dapat diperlakukan sebagai kekuatan netral yang memantau dan harus bekerja sama dengan Board of Peace untuk memastikan gencatan senjata tetap terjaga. Selain itu, Otoritas Palestina dan Organisasi Pembebasan Palestina tampaknya tidak memiliki peran dalam rencana yang diusulkan; resolusi tersebut hanya menyebutkan pasukan polisi Palestina yang baru dilatih dan diverifikasi

“Mahkamah Internasional (ICJ) telah menegaskan: penentuan nasib sendiri adalah hak yang tidak dapat dicabut dari rakyat Palestina dan PBB serta semua negara memiliki kewajiban untuk membantu mewujudkannya. Hal ini hanya dapat dimulai dengan penarikan segera dan tanpa syarat dari kehadiran Israel yang melanggar hukum di wilayah Palestina yang diduduki.”

Sementara menurut para Pelapor Khusus PBB pembentukan Board of Peace tidak memiliki legalitas dalam hukum HAM internasional:²⁸⁰

“Sebagai agresor dan kekuatan pendudukan, tanggung jawab ini dimulai pertama dan terutama Israel dan negara-negara yang memberikan dukungan militer dan dukungan lainnya untuk kampanyenya di Gaza. Gencatan senjata harus dipertahankan, pendudukan harus diakhiri, dan harus ada jaminan untuk tidak terulangnya hal serupa sebagai prasyarat untuk setiap proses rekonstruksi yang berkelanjutan dan berbasis HAM. Pembentukan Dewan Perdamaian adalah manuver ilegal dan tidak sah oleh negara-negara kuat yang didorong oleh nostalgia dan keserakahan,”

Namun demikian, Presiden Prabowo Subianto justru melihat dengan perspektif yang berbeda. Kehadiran Indonesia menjadi peluang untuk mencapai kemerdekaan bagi Palestina. Presiden Prabowo Subianto melihat keanggotaan di Dewan Perdamaian (Board of Peace) sebagai upaya mencapai perdamaian di Gaza, Palestina. Presiden Prabowo se usai penandatanganan piagam di Davos, Swiss pada Kamis, 22 Januari 2026 menyatakan:²⁸¹

tanpa menyatakan siapa dan bagaimana mereka akan dibentuk, dan badan politik Palestina mana yang mereka ikuti. Dengan kata lain, resolusi tersebut menyerukan untuk melegitimasi pendudukan Israel di Jalur Gaza dan mendelegitimasi Otoritas Palestina, Organisasi Pembebasan Palestina, dan hak penentuan nasib sendiri rakyat Palestina. Hal ini melanggar Pasal 24(2) Piagam PBB yang menyatakan: “Dewan Keamanan Harus Bertindak Sesuai Prinsip-Prinsip Piagam.” Dewan Keamanan PBB bertindak di luar kewenangannya dengan mengadopsi rencana komprehensif Donald Trump yang mengecualikan Palestina dan memasukkan penjajah mereka. Lihat, Yousef, “Why the Recent UNSC Resolution 2803 ‘Board of Peace’ Violates the UN Charter.”

²⁸⁰ Para ahli HAM PBB tersebut (1) Balakrishnan Rajagopal, Pelapor Khusus tentang perumahan yang layak sebagai komponen hak atas standar hidup yang layak, dan tentang hak untuk tidak diskriminasi dalam konteks ini; (2) Francesca Albanese, Pelapor Khusus tentang situasi HAM di wilayah Palestina yang diduduki sejak 1967; (3) Cecilia M. Bailliet, Pakar Independen tentang hak asasi manusia dan solidaritas internasional; (4) George Katrougalos, Pakar Independen tentang promosi tatanan internasional yang demokratis dan adil; (5) Paula Gaviria, Pelapor Khusus tentang hak asasi manusia pengungsi internal; (6) Pedro Arrojo-Agudo, Pelapor Khusus tentang hak asasi manusia atas air minum yang aman dan sanitasi; (7) Michael Fakhri, Pelapor Khusus tentang hak atas pangan; dan (8) Margaret Satterthwaite, Pelapor Khusus tentang independensi hakim dan advokat. Lihat, Office of the United Nations High Commissioner for Human Rights (OHCHR), “UN Experts Condemn ‘Board of Peace,’ Call for a Reparative, Rights-Based Approach to Reconstruction in Gaza,” <https://www.ohchr.org/en/special-procedures/sr-housing/mr-balakrishnan-rajagopal>.

²⁸¹ Tempo, “Prabowo Ungkap Alasan Gabung Dewan Perdamaian Bentuk Trump,” 23 Januari 2026, <https://www.tempo.co/politik/prabowo-ungkap-alasan-gabung-dewan-perdamaian-bentukan-trump-2109216>.

"Saya kira ini kesempatan bersejarah. Ini benar-benar peluang untuk mencapai perdamaian di Gaza. Saya sangat berharap dan Indonesia siap ikut serta. Siapa yang ingin perdamaian di situ, siapa yang ingin bantu rakyat Gaza, rakyat Palestina

Bahkan Presiden Prabowo Subianto mengklaim saat ini situasi di Gaza telah membaik setelah agresi Israel yang berlangsung sejak 2023.

"Yang jelas, penderitaan rakyat Gaza sudah berkurang, sangat berkurang ya. Sangat berkurang."

Pembentukan Board of Peace penting untuk diletakkan dalam konteks Pelapor Khusus tentang situasi HAM di wilayah Palestina yang diduduki sejak tahun 1967, Francesca Albanese. Laporan terbaru yang terbit pada 20 Oktober 2025, *Genosida Gaza: Kejahatan Kolektif (Gaza Genocide: A Collective Crime)*. Francesca Albanese, menunjukkan dalam laporan tersebut bahwa genosida yang sedang berlangsung terhadap warga Palestina harus dipahami sebagai kejahatan yang didukung secara internasional. Banyak negara ketiga telah memfasilitasi, melegitimasi, dan pada akhirnya menormalisasi kampanye genosida yang dilakukan oleh Israel. Menurut Pelapor Khusus, negara ketiga telah mereproduksi distorsi hukum internasional dan kiasan kolonial Israel, berupaya membenarkan keterlibatan mereka sendiri dalam genosida.²⁸²

Pelapor Khusus mengidentifikasi empat komponen yang saling terkait dalam genosida rakyat Palestina di Gaza yakni diplomatik, militer, ekonomi, dan kemanusiaan. Keempat komponen ini dapat diuraikan secara ringkas, sebagai berikut: (1) genosida yang berkedok tindakan diplomatik dan politik; (2) hubungan militer yang menyediakan sarana penghancuran; (3) persenjataan bantuan (*weaponization of aid*) yang menciptakan kondisi hidup untuk genosida; dan (4) hubungan ekonomi dan perdagangan, khususnya bahan bakar dan keuntungan dari genosida. Menurut Pelapor Khusus Indonesia memiliki peran dalam tindak diplomatik dan politik,²⁸³ khususnya dukungan Indonesia²⁸⁴ atas pembentukan Board of Peace:

²⁸² Francesca Albanese, *Report of the Special Rapporteur on the Situation of Human Rights in the Palestinian Territories Occupied since 1967: Gaza Genocide: A Collective Crime*, A/80/492 (New York: United Nations, 20 Oktober 2025).

²⁸³ Dukungan politik dan diplomatik yang berkepanjangan dari negara-negara ketiga yang berpengaruh telah memungkinkan Israel untuk memulai dan mempertahankan serangannya terhadap rakyat Palestina. Dalam dua tahun terakhir, keterlibatan yang mengakar ditandai dengan memanipulasi narasi dan mereproduksi kebohongan Israel telah membunkam seruan mendesak untuk bertindak dan mengaburkan peranan jalinan kepentingan politik, keuangan, dan militer. Kegagalan yang telah berlangsung lama untuk mengatasi pelanggaran berat hukum internasional oleh Israel telah menormalisasi, memperdalam dan memperkuat penindasan, dominasi, dan penghapusan rakyat Palestina. Lihat, Albanese, *Gaza Genocide: A Collective Crime*.

²⁸⁴ Beberapa poin penting Pernyataan Bersama Menteri Luar Negeri Yordania, Uni Emirat Arab, Indonesia, Pakistan, Turki, Arab Saudi, Qatar, dan Mesir, sebagai berikut: 1) Menyambut kepemimpinan

Pada 30 September 2025, banyak negara, termasuk Mesir, Indonesia, Yordania, Pakistan, Qatar, Arab Saudi, Turki, dan Uni Emirat Arab mendukung Trump Plan (Rencana Trump) meskipun rencana tersebut tidak menyinggung soal pengakhiran pendudukan, penjaminan akuntabilitas, maupun penyediaan keadilan transisi, serta memaksakan mekanisme tata kelola asing yang bersifat imperial bagi Gaza yang justru semakin melemahkan alih-alih mewujudkan hak penentuan nasib sendiri rakyat Palestina;

Laporan tersebut menemukan hubungan ekonomi dan perdagangan juga berkontribusi terhadap terjadinya genosida di Gaza. Transaksi piranti *spyware* antara Indonesia dengan Israel meskipun melalui perantara pihak ketiga dalam rantai pasokan teknologi dwiguna akan memperkuat kapasitas Israel dalam memproduksi teknologi dwiguna. Laporan Pelapor Khusus menyebutkan:²⁸⁵

Banyak impor Israel adalah barang-barang dwiguna, yang dapat digunakan dalam produksi produk sipil dan militer. Sering dipasarkan sebagai teknologi sipil, barang-barang dwiguna ini sangat penting bagi sistem militer Israel yang memata-matai, mengendalikan, dan membunuh warga Palestina, memperkuat simbiosis ekonomi militer-sipil dan peran negara tersebut dalam perlombaan senjata teknologi global.

Impor teknologi dwiguna dari Israel dalam dikerangkai melalui pandangan Gráinne de Búrca dan Katherine Young sebagai bentuk penyalahgunaan (mis-apropriasi) HAM (*misappropriations of human rights*). Mis-apropriasi HAM merujuk pada praktik penggunaan bahasa HAM, namun untuk melayani tujuan yang bersifat eksklusif, represif, atau anti-pluralis.²⁸⁶ Dalam kaitan ini, menurut Kristina Stoeckl, pengambilalihan hak (*rights appropriation*) bukanlah sesuatu yang spesifik bagi kelompok aktor dan pandangan dunia ideologis tertentu, melainkan, semua makna HAM dibangun dalam

Presiden Donald J. Trump dan upaya tulusnya untuk mengakhiri perang di Gaza, dan menegaskan kepercayaan mereka pada kemampuannya untuk menemukan jalan menuju perdamaian. 2) Menegaskan kesediaan mereka untuk terlibat secara positif dan konstruktif dengan Amerika Serikat dan para pihak dalam menyelesaikan perjanjian dan memastikan pelaksanaannya, dengan cara yang menjamin perdamaian, keamanan, dan stabilitas bagi rakyat di kawasan tersebut. 3) Menegaskan kembali komitmen bersama mereka untuk bekerja sama dengan Amerika Serikat untuk mengakhiri perang di Gaza melalui kesepakatan komprehensif yang memastikan pengiriman bantuan kemanusiaan yang cukup ke Gaza tanpa batasan, tidak ada pengusiran warga Palestina, pembebasan sandera, mekanisme keamanan yang menjamin keamanan semua pihak, penarikan penuh Israel, pembangunan kembali Gaza, dan menciptakan jalan menuju perdamaian yang adil berdasarkan solusi dua negara, di mana Gaza sepenuhnya terintegrasi dengan Tepi Barat dalam negara Palestina sesuai dengan hukum internasional sebagai kunci untuk mencapai stabilitas dan keamanan regional. Lihat, Ministry of Foreign Affairs of Pakistan, "Joint Statement by the Foreign Ministers of Jordan, United Arab Emirates, Indonesia, Pakistan, Türkiye, Saudi Arabia, Qatar and Egypt," <https://mofa.gov.pk/press-releases/joint-statement-by-the-foreign-ministers-of-jordan-united-arab-emirates-indonesia-pakistan-turkiye-saudi-arabia-qatar-and-egypt>.

²⁸⁵ Albanese, *Gaza Genocide: A Collective Crime*.

²⁸⁶ Gráinne de Búrca dan Katharine G. Young, "The (Mis)appropriation of Human Rights by the New Global Right: An Introduction to the Symposium," *International Journal of Constitutional Law* 21, no. 1 (Januari 2023).

praktik sosial dan politik yang konkret. Semua aktor yang terlibat dalam tindakan dan politik seputar HAM dengan satu atau lain cara menjadikan hak-hak tersebut milik mereka sendiri (make rights their own) dan mengisi ketentuan HAM dengan makna yang dikontekstualisasikan. Kemudian Kristina Stoeckl mengakui bahwa beberapa pengambilalihan HAM dapat memiliki efek eksklusif dan represif, terutama ketika hal itu memperkuat ketidakseimbangan kekuasaan yang ada dan memarginalkan orang-orang yang rentan.²⁸⁷

7. Irisan Kebangkitan Militerisasi dan Penggunaan Teknologi Dwi Guna: Identifikasi Dampaknya Terhadap HAM

Meskipun Indonesia telah memasuki era demokrasi Pasca-1998, jejak keterlibatan aktif militer masih terlihat secara kentara. Keterlibatan militer yang diarahkan untuk mendorong partisipasi pemilih bukanlah hal yang luar biasa maupun kebetulan semata. Sebaliknya, hal itu merupakan respons terhadap kekhawatiran presiden petahana saat itu, Joko Widodo. Berdasarkan kalkulasi Presiden Joko Widodo rendahnya partisipasi pemilih dapat mengancam peluangnya untuk terpilih kembali. Kampanye militer tersebut membuahkan hasil: tingkat partisipasi pemilih dalam pemilihan presiden tahun 2019 mencapai 79%, angka yang jauh lebih tinggi dibandingkan pemilihan umum sebelumnya pada tahun 2014, bahkan merupakan angka tertinggi sejak dimulainya pemilihan presiden secara langsung pada tahun 2004.²⁸⁸ Hal ini menunjukkan bahwa sistem presidensialisme koalisional baru di Indonesia yang menurut Marcus Mietzner memungkinkan militer memulihkan sebagian kekuasaannya. Hal ini terjadi karena militer menempatkan diri sebagai elemen penting dalam koalisi presidensial, serta memanfaatkan pandangan sebagian besar presiden mengecualikan militer dari pembagian kekuasaan akan membuat pemerintahan sipil menjadi tidak stabil. Sistem presidensial koalisional menunjukkan bagaimana hubungan sipil-militer di Indonesia

²⁸⁷ Saskia Schäfer dan Daniel Peterson, "Appropriations of Human Rights Discourses: Evidence from Indonesia and Malaysia," *International Journal of Constitutional Law* 24, no. 1 (Januari 2026).

²⁸⁸ Lingkaran Presiden Joko Widodo telah mengidentifikasi rendahnya tingkat partisipasi pemilih sebagai ancaman terbesar bagi kampanye untuk memenangkan kembali kursi kepresidenan. Untuk itu, Presiden Joko Widodo mengambil langkah-langkah sistematis dengan melibatkan militer. Wiranto, selaku Menteri Koordinator Bidang Politik, Hukum, dan Keamanan pada Maret 2019 melontarkan ancaman bahwa pihak-pihak yang menganjurkan golput dapat dijerat dengan undang-undang antiterorisme. Milite mengambil tindakan serupa meluncurkan kampanye untuk mendorong pemilih agar datang ke tempat pemungutan suara. Bahkan banyak poster yang disebar di seluruh penjuru Indonesia memasang gambar Panglima TNI saat itu, Marsekal Hadi Tjahjanto dan Kapolri Jenderal Tito Karnavian. Lihat, Marcus Mietzner, "The Military's Transformation from Praetorian Ruler to Presidential Coalition Partner," dalam *Oxford Research Encyclopedia of Politics*, ed. Erin Hannah (New York: Oxford University Press, 2020).

sangat dipengaruhi oleh relasi khusus yang dijalin presiden dengan lingkungan politik di sekitarnya.²⁸⁹

Di bawah Pemerintahan Presiden Joko Widodo pada 2019, militer telah mengukuhkan posisi politiknya sebagai elemen penting dalam koalisi kepresidenan. Namun demikian, militer tidak lagi memiliki sarana maupun wewenang untuk membentuk lanskap politik dan kekuasaan militer berfluktuasi menyesuaikan dengan dinamika koalisi presidensialisme, baik itu partai politik maupun aktor negara yang berpengaruh. Namun demikian, dinamika politik yang ada memperlihatkan peran militer tetap memiliki relevansi politik dan tidak mengalami depolitisasi sebagaimana diharapkan oleh para reformis sipil pasca-perubahan rezim tahun 1998. Hal ini berarti militer kini menjadi salah satu dari sekian banyak pelaku dalam dinamika politik Indonesia pasca-otoritarianisme yang kompleks.²⁹⁰ Menurut Muhammad Haripin untuk merespons situasi politik yang tidak stabil Presiden Joko Widodo mengambil strategi politik dengan menjalin aliansi politik bersama militer, dan sampai batas tertentu dengan kepolisian. Presiden Joko Widodo menempatkan peran militer sebagai kekuatan penyeimbang terhadap tekanan oposisi politik.²⁹¹

Kebangkitan kembali militer dalam kancah politik yang merupakan manifestasi ide dan praktik era Orde Baru tidak terlepas dari peran Joko Widodo. Joko Widodo membingkai praktik politik dengan karakteristik pemerintahan Orde Baru, seperti developmentalism, penindasan, persaingan yang terbatas, akuntabilitas yang lemah, dan sentralisasi kekuasaan negara. Joko Widodo merupakan tokoh yang memikul tanggung jawab utama atas kemunduran demokrasi, termasuk menguatnya militerisasi yang menjadi benih pertumbuhan rezim Orde Baru. Menurut Sana Jaffrey dan Eve Warburton terdapat dua ciri utama kepresidenan Joko Widodo (1) kembalinya developmentalisme di bidang ekonomi; dan (2) kebangkitan otoritarianisme di bidang politik.²⁹² Pelemahan Komisi Pemberantasan Korupsi (KPK); penyusunan Kitab Undang-Undang Hukum Pidana (KUHP) baru yang menjadikan kritik terhadap pejabat publik sebagai tindak pidana; serta

²⁸⁹ Selain faktor sistem presidensialisme koalisional, faktor-faktor pendorong politisasi dan depolitisasi militer di Indonesia juga dipengaruhi tiga pola lain, yaitu: (1) peran kunci masa revolusi dalam memperkuat keyakinan militer bahwa militer tetap berhak memiliki peran politik, sekaligus dalam melahirkan doktrin militer yang mendasari klaim tersebut; (2) konflik internal di kalangan sipil serta kelemahan-kelemahan lain dalam politik demokratis yang menjadi faktor penarik bagi kiprah politik militer, baik pada pertengahan tahun 1950-an, tahun 1960-an, maupun pada masa transisi segera pasca 1998; dan (3) keberhasilan politisi sipil dalam menjaga stabilitas ekonomi dan politik secara umum, seperti pada awal 1950-an atau setelah tahun 2004, memberikan jaminan terbaik untuk membendung ambisi politik militer. Lihat, Mietzner, "The Military's Transformation from Praetorian Ruler."

²⁹⁰ Mietzner, "The Military's Transformation from Praetorian Ruler."

²⁹¹ Muhamad Haripin dan Adhi Priamarizki, "Jokowi Consolidates Influence over TNI as Elections Loom," *New Mandala*, <https://www.newmandala.org/jokowi-consolidates-influence-over-tni-as-elections-loom/>.

²⁹² Sana Jaffrey dan Eve Warburton, "Introduction: Jokowi's Decade in Power," dalam *The Jokowi Presidency: Indonesia's Decade of Authoritarian Revival*, ed. Sana Jaffrey dan Eve Warburton (Singapore: ISEAS–Yusof Ishak Institute, 2025).

Undang-Undang Omnibus tentang Cipta Kerja yang melucuti perlindungan bagi pekerja dan ketentuan pelestarian lingkungan. Hal ini memperkuat penanaman pola-pola otoriter dalam wacana dan praktik politik selama Kepemimpinan Joko Widodo. Lebih jauh, Joko Widodo membungkam oposisi dari aktor masyarakat sipil dengan tindakan represi secara sistematis untuk mempersempit ruang ekspresi perbedaan pendapat yang sah.²⁹³ Kemudian, Ken Setiawan menyatakan pemerintahan Joko Widodo telah mempersenjatai diri melalui surveilans online dan intimidasi untuk menakut-nakuti lawan politik dan menghambat kritik publik. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU TIK), digunakan untuk membungkam kritik dari lawan politik, jurnalis, aktivis, dan warga biasa.²⁹⁴ Hal ini menunjukkan, Indonesia seperti halnya Rusia,²⁹⁵ termasuk di antara banyak negara yang mengendalikan internet melalui mekanisme hukum dan teknis. Seperti halnya Rusia, Indonesia telah menetapkan undang-undang dan panduan teknis selama bertahun-tahun untuk mengendalikan informasi online. Penerapan pengendalian, seperti pemblokiran konten, di Indonesia bersifat terdesentralisasi. Artinya, meskipun pemerintah menetapkan pedoman mengenai konten apa yang harus diblokir pelaksanaan teknisnya diserahkan kepada diskresi masing-masing penyedia layanan internet. Kerangka legislasi, seperti Undang-Undang tentang Informasi dan Transaksi Elektronik dan Undang-Undang tentang Pornografi sering kali dijadikan dasar pembenaran bagi pengendalian internet.²⁹⁶ Pendekatan kontrol internet secara teknis menghadirkan tantangan karena, tidak seperti kerangka hukum yang lebih mudah dipahami publik, metode teknis cenderung tidak

²⁹³ Ketidaktoleranan Joko Widodo terhadap perbedaan pendapat mendapatkan dukungan dari sekutunya di DPR dan diformalkan pada 2022 sebagai bagian dari KUHP Indonesia yang baru, yang memuat hukuman berat, termasuk hukuman penjara, bagi siapa pun yang mengkritik pejabat publik. Salah satu faktor penting yang memungkinkan Joko Widodo untuk menekan kelompok masyarakat sipil berkaitan dengan keberadaan kepolisian yang berada dalam pengaruh kekuasaannya. Menurut Sidney Jones selama sepuluh tahun pemerintahan Joko Widodo, kepolisian hampir menjadi 'perpanjangan kekuasaan pribadinya. Lebih jauh, Sidney Jones menunjukkan Joko Widodo banyak belajar pentingnya aktor keamanan, khususnya kepolisian sebagai instrumen politik untuk melindungi sekutu dan mengintimidasi lawan. Bagi seorang tokoh populis, maka memerlukan upaya membendung ancaman politik. Aktor keamanan menjadi sekutu yang sangat penting untuk memelihara kekuasaan. Lihat, Jaffrey dan Warburton, "Introduction: Jokowi's Decade in Power."

²⁹⁴ Ken M. P. Setiawan, "A State of Surveillance? Freedom of Expression under the Jokowi Presidency," dalam *Democracy in Indonesia: From Stagnation to Regression?*, ed. Thomas Power dan Eve Warburton (Singapore: ISEAS–Yusof Ishak Institute, 2020).

²⁹⁵ Rusia telah mengesahkan undang-undang yang memfasilitasi pengendalian internet yang diarahkan oleh negara sekaligus membebaskan kewajiban teknis kepada perantara informasi. Regulator internet negara tersebut, Roskomnadzor, menegakkan undang-undang ini dan telah menerbitkan serangkaian rekomendasi teknis terperinci bagi Penyedia Layanan Internet (ISP) untuk menyaring atau memblokir konten online. Ketidakpatuhan berujung pada sanksi, seperti denda. Pengendalian internet di Indonesia tidak dilakukan dengan cara mengoperasikan sistem penyaringan teknis berskala nasional seperti sistem penyaringan Great Firewall milik China, namun diserahkan pada penyedia layanan internet yang memiliki kapasitas dan kemampuan teknis. Lihat Irene Poetranto, "Techno-Legal Internet Controls in Indonesia and Their Impact on Free Expression," dalam *Digital Democracy in a Divided Global Landscape* (Washington, DC: Carnegie Endowment for International Peace, 2025), 35–38.

²⁹⁶ Poetranto, "Techno-Legal Internet Controls in Indonesia."

terlihat jelas dan memerlukan pengetahuan atau keahlian khusus untuk memahaminya. Penerapan kontrol yang diterapkan melalui infrastruktur internet atau sarana teknis berdampak pada kebebasan berekspresi dan akses terhadap informasi. Selain itu, seiring pemerintah bereksperimen dengan berbagai metode teknis untuk mengontrol internet yang berpotensi menghambat arus informasi online.²⁹⁷

Penyusutan ruang sipil yang dramatis pada masa Pemerintahan Presiden Joko Widodo ini terlihat melalui penerapan Undang-Undang tentang informasi dan transaksi elektronik yang sebagai salah satu senjata utama yang digunakan pemerintah untuk menyasar lawan-lawannya. Penyalahgunaan UU ITE oleh pemerintah tampaknya membuahkan hasil sesuai tujuan mereka. Sudah ada bukti nyata mengenai munculnya efek gentar (*chilling effect*) di tengah masyarakat Indonesia.²⁹⁸

Surveilans negara diperkuat melalui pembentukan Unit Siber oleh Kepolisian RI pada 2021 untuk memperluas jangkauan dan kemampuan pengawasan media sosial dengan bantuan piranti spyware. Kemudian Pemerintah juga mempersenjatai diri melalui Peraturan Menteri Nomor 5 Tahun 2020 yang mewajibkan layanan dan platform digital swasta untuk mendaftar ke Kementerian Komunikasi dan Informatika serta menyerahkan data pengguna pribadi kepada instansi pemerintah. Dengan demikian, sarana-sarana ini dapat digunakan untuk memantau aktivis masyarakat sipil dan jurnalis.²⁹⁹ Laporan Amnesty International memperkuat upaya pengawasan negara yang mengancam kebebasan dan hak dasar warga negara, khususnya pengguna teknologi.³⁰⁰

Jumlah penjualan dan penyebaran *spyware* yang sangat invasif yang teridentifikasi di Indonesia sangat mengkhawatirkan. Pada sisi yang lain ruang sipil telah menyusut dalam beberapa tahun terakhir karena serangan berkelanjutan terhadap hak

²⁹⁷ Citizen Lab mengidentifikasi hingga tahun 2024, sebagian besar penyedia layanan internet di Indonesia menerapkan pemblokiran menggunakan metode apa pun yang mereka anggap sesuai. Salah satu kemungkinan penyebabnya adalah bahwa pengalihan Domain Name System (DNS) lebih mahal dan lebih sulit diterapkan oleh penyedia layanan internet dibandingkan bentuk manipulasi DNS lainnya. Perantara informasi sering kali bertanggung jawab atas penerapan kontrol internet, dan mandat teknis untuk memblokir, mengawasi, atau mengalihkan lalu lintas internet berdasarkan permintaan Pemerintah. Lihat, Poetranto, "Techno-Legal Internet Controls in Indonesia."

²⁹⁸ Survei tahun 2022 yang dilakukan Indikator Politik, menunjukkan bahwa 62,9 persen masyarakat Indonesia merasa takut untuk mengungkapkan pendapat mereka secara terbuka. Senada dengan itu, survei pada Oktober 2024 oleh Saiful Mujani Research and Consulting (SMRC) menemukan bahwa menjelang akhir masa jabatan 10 tahun Presiden Joko Widodo, terdapat 51 persen responden merasa takut untuk membicarakan politik. Angka ini menunjukkan peningkatan signifikan dibandingkan tahun 2014 saat Joko Widodo mulai menjabat, di mana hanya 22 persen masyarakat Indonesia yang mengaku takut membahas politik. Lihat, Tim Mann, "Activists on Trial: The Weaponisation of Online Defamation Provisions in Indonesia," *Australian Journal of Asian Law* 25, no. 2 (2025): 1–16.

²⁹⁹ Andreas Ufen, "The Rise of Digital Repression in Indonesia under Joko Widodo," *GIGA Focus Asia*, no. 1 (Januari 2024), <https://doi.org/10.57671/gfas-24012>.

³⁰⁰ Amnesty International, *A Web of Surveillance*.

kebebasan berekspresi, berkumpul dan berasosiasi secara damai, keamanan pribadi, dan kebebasan dari penahanan sewenang-wenang.

Kemudian, Presiden Joko Widodo juga memanfaatkan perangkat intelijen menjadikan partai politik sebagai pilar demokrasi menjadi objek dan target pengawasan. Tindakan ini selain mengindikasikan penyalahgunaan kekuasaan, surveilans tersebut merusak demokrasi, melemahkan supremasi hukum, dan mengancam HAM.³⁰¹ Pemanfaatan data intelijen ini merupakan manifestasi dari pernyataan Presiden Joko Widodo yang akan ikut campur dalam pemilu dengan dalih demi kebaikan bangsa. Pemanfaatan data intelijen dapat disalahgunakan untuk menopang kepentingan elektoralnya dalam Pemilu 2024 untuk mendukung pencalonan Gibran Rakabuming Raka sebagai pendamping Prabowo Subianto.³⁰²

Menurut Muhamad Haripin, pernyataan Presiden Joko Widodo memperlihatkan hubungan antara presiden dan lembaga intelijen yang penuh dengan konflik kepentingan. Presiden Joko Widodo dinilai tengah melakukan praktik spionase politik terkait pernyataannya yang mengaku memiliki data intelijen terkait kondisi internal dan agenda partai politik. Penyalahgunaan data intelijen tersebut tidak terlepas dari tiga permasalahan mendasar terkait hubungan antara presiden dan lembaga intelijen, yakni kelemahan regulasi, konflik kepentingan, dan kompleksitas ancaman. Pernyataan Presiden Joko Widodo yang memiliki data intelijen kondisi internal dan agenda partai politik (parpol) memperlihatkan adanya konflik kepentingan, terkait hubungan presiden dengan lembaga intelijen.³⁰³ Kasus serangan siber yang menargetkan Menteri Koordinator Bidang Perekonomian, Airlangga Hartarto, yang diduga disponsori negara, dapat dilihat dalam konteks ini. Pesan email dari Apple Inc pada November 2021 yang menyatakan bahwa Apple mengidentifikasi beberapa individu pejabat sedang menjadi target serangan yang disponsori negara.³⁰⁴ Pemanfaatan *spyware* yang disponsori negara membuktikan adanya penyalahgunaan kuasa oleh presiden untuk memanfaatkan kapasitas lembaga intelijen untuk kepentingan politik presiden.

³⁰¹ Tempo, "Jokowi Pamer Pegang Data Intelijen Arah Parpol, Begini Bunyi Pasal 1 dan 2 UU Nomor 17 Tahun 2011 tentang Intelijen Negara," 20 September 2023, <https://www.tempo.co/politik/jokowi-pamer-pegang-data-intelijen-arrah-parpol-begini-bunyi-pasal-1-dan-2-uu-nomor-17-tahun-2011-tentang-intelijen-negara-141871>.

³⁰² Haripin dan Priamarizki, "Jokowi Consolidates Influence over TNI."

³⁰³ Aryo Putranto Saptohutomo, "Jokowi Dinilai Lakukan Intelijen Politik saat Kantongi 'Rahasia' Parpol," *Kompas.com*, 22 September 2023, <https://nasional.kompas.com/read/2023/09/22/06000011/jokowi-dinilai-lakukan-intelijen-politik-saat-kantongi-rahasia-parpol?page=all>.

³⁰⁴ Target serangan ditujukan kepada Menteri Perekonomian Utama Airlangga Hartarto, personel militer senior, dua diplomat regional, dan penasihat di kementerian pertahanan dan luar negeri Indonesia. Lihat, target serangan termasuk Menteri Perekonomian Utama Airlangga Hartarto, personel militer senior, dua diplomat regional, dan penasihat di kementerian pertahanan dan luar negeri Indonesia., Reuters, "Indonesian Officials Targeted by Spyware: Sources," *Al Jazeera*, 30 September 2022, <https://www.aljazeera.com/economy/2022/9/30/indonesian-officials-targeted-by-spyware-sources>.

Keterpilihan Prabowo Subianto sebagai presiden pada Pemilu 2024 menandai berakhirnya demokrasi liberal di Indonesia dan kembalinya model pemerintahan Orde Baru. Pembongkaran pilar-pilar demokrasi liberal di Indonesia yang telah dilakukan oleh Presiden Joko Widodo memudahkan kembalinya doktrin dwi fungsi yang menjadi pilar utama Orde Baru melalui amandemen UU tentang Aparat Sipil Negara dan UU tentang Tentara Nasional Indonesia.³⁰⁵ Konsekuensi lebih jauh, Presiden Prabowo Subianto mulai membangunkan kembali era praetorianisme ala Orde Baru dengan cara memperluas kapasitas dan jangkauan pengaruh politik militer ke ranah kehidupan sipil. Hal ini paling tidak terindikasi dari diresmikannya 162 satuan baru, termasuk di dalamnya enam komando daerah militer (kodam) dan melantik sejumlah perwira tinggi oleh Presiden Prabowo Subianto. Penambahan satuan baru dan perwira tinggi sebagai tindak lanjut Peraturan Presiden (Perpres) Nomor 84 Tahun 2025 yang merevisi Perpres No 66/2019. Perpres baru mengatur 420 jabatan perwira tinggi bertambah 49 dari sebelumnya. Regulasi yang melegalisasi penempatan perwira militer mengisi jabatan publik diperkuat melalui Undang-Undang No 3/2025 tentang Perubahan atas UU No 34/2004 tentang Tentara Nasional Indonesia. Presiden Prabowo Subianto hendak membangun infrastruktur teritorial yang berpotensi menjadi saluran pengaruh politik hingga tingkat desa, mengulang fungsi militer pada era Orde Baru. Langkah politik Presiden Prabowo Subianto ini menurut Dwi Munthaha mengarah pada manifestasi *military pretorian-entrepreneur* karena militer tidak hanya terlibat dalam politik, tetapi juga menguasai jaringan bisnis dan sumber daya publik.³⁰⁶

Fenomena *military pretorian-entrepreneur* dapat dilihat dari pelaksanaan MBG dan Koperasi Merah Putih. Pelaksanaan TNI dalam MBG terlihat antara lain dalam peresmian 339 Satuan Pelayanan Pemenuhan Gizi (SPPG) oleh panglima TNI di Lanud Adi Soemarmo, Jawa Tengah, pada 26 September 2025. Dengan peresmian itu, total SPPG yang berada di bawah TNI mencapai 452 unit di seluruh Indonesia.³⁰⁷

Pada saat yang sama, TNI juga terlibat pelaksanaan program koperasi merah putih melalui penandatanganan kerja sama antara PT Agrinas Pangan Nusantara dan TNI pada 10 Oktober 2025.³⁰⁸ Kesepakatan itu memuat kewenangan militer untuk ikut

³⁰⁵ Tim Lindsey, "Indonesia's New President, Prabowo Subianto, Finds Democracy 'Very Tiring'. Are Darker Days Ahead for the Country?," *The Conversation*, 18 Oktober 2024, <https://theconversation.com/indonesias-new-president-prabowo-subianto-finds-democracy-very-tiring-are-darker-days-ahead-for-the-country-241256>.

³⁰⁶ Dwi Munthaha, "Militer Era Prabowo: Pretorianisme Baru?," *Kompas.id*, 20 Agustus 2025, <https://www.kompas.id/artikel/militer-era-prabowo-pretorianisme-baru>.

³⁰⁷ Kepala Staf Tentara Nasional Indonesia (TNI) Angkatan Darat Jenderal Maruli Simanjuntak menjelaskan alasan TNI terlibat luas dalam Program MBG didorong oleh kebutuhan memperkuat dampak sosial dan ekonomi program tersebut. KSAD Jelaskan Alasan TNI Banyak Terlibat dalam Program MBG Lihat, *Tempo*, "KSAD Jelaskan Alasan TNI Banyak Terlibat dalam Program MBG," 10 November 2025, <https://www.tempo.co/politik/ksad-jelaskan-alasan-tni-banyak-terlibat-dalam-program-mbg-2087989>.

³⁰⁸ *Tempo*, "Koperasi Desa Merah Putih," *Tempo.co*, <https://www.tempo.co/tag/koperasi-desa-merah-putih>.

terlibat mempercepat pembangunan gedung koperasi di daerah. Pelibatan ini juga dilandasi Surat Edaran Nomor 4 Tahun 2025 tentang Pendataan Aset Tanah dan Bangunan untuk Percepatan Koperasi Merah Putih yang diterbitkan oleh Menteri Koperasi. Salah satu poinnya, perangkat desa mesti berkoordinasi dengan komando distrik militer setempat dalam pendataan aset berupa tanah dan bangunan. Komandan di satuan wilayah setempat lantas akan melaporkan data aset ke PT Agrinas Pangan.³⁰⁹

Jejak keterlibatan militer dalam urusan ekonomi nampak pada saat periode kepemimpinan Presiden Soeharto pada akhir tahun 1960-an serta sepanjang sebagian besar tahun 1970-an. Penggalan periode tersebut merupakan contoh klasik negara praetorian. Militer mendominasi seluruh cabang pemerintahan, memperketat kendali atas masyarakat, dan melakukan intervensi mendalam dalam perekonomian di Indonesia.³¹⁰ Instrumentasi dan infrastruktur baru pengaruh politik dan ekonomi TNI baru tersebut, semakin diperkuat kembali melalui perluasan kewenangan TNI untuk terlibat dalam urusan di luar bidang pertahanan (*operasi militer selain perang*) untuk memasuki ranah siber.³¹¹

Undang-Undang Nomor 3 Tahun 2025 tentang Perubahan Atas UU Nomor 34 Tahun 2004 tentang TNI secara substantif memuat perubahan yang signifikan termasuk perluasan kewenangan. Menurut Muhammad Haripin signifikansi revisi UU tentang TNI, terlihat pada beberapa dimensi:³¹²

Pertama, revisi UU tentang TNI tersebut memungkinkan perluasan operasi militer TNI selain perang (*military operations other than war*), dengan menambahkan dua misi tambahan, yaitu misi pertahanan siber dan perlindungan warga negara Indonesia dan kepentingan nasional di luar negeri,³¹³

³⁰⁹ Tempo, "Cerita Kepala Desa soal Peran Tentara di Kopdes Merah Putih," 16 Februari 2026, <https://www.tempo.co/politik/cerita-kepala-desa-soal-peran-tentara-di-kopdes-merah-putih-2115459>.

³¹⁰ Mietzner, "The Military's Transformation from Praetorian Ruler."

³¹¹ Terdapat harapan global peran militer, termasuk TNI di Indonesia mampu menjalankan peran beragam di luar peperangan konvensional melawan musuh asing dan misi kontra-pemberontakan. Perluasan peran ini menghadirkan tantangan yang kompleks. Berbeda dengan peperangan konvensional atau konflik bersenjata antarnegara, standar keberhasilan misi pemeliharaan perdamaian atau stabilitas, misi kemanusiaan dan penanggulangan bencana, serta kontra-terorisme sulit untuk ditakar sejauhmana keberhasilan operasi tersebut. Lihat Muhamad Haripin, *Civil-Military Relations in Indonesia: The Politics of Military Operations Other Than War* (Abingdon: Routledge, 2020).

³¹² Revisi tersebut juga memperpanjang usia pensiun bagi personel militer yang justru akan mengganggu siklus regenerasi personel sehingga menyebabkan ketidakseimbangan pada struktur piramida hierarki militer. Lihat, Muhamad Haripin, "Indonesian Parliament Passes Law Expanding Military's Role in Government," *ADRN Issue Briefing*, 17 April 2025, <http://adrnresearch.org/publications/list.php?cid=2&idx=407&ckattempt=3>.

³¹³ Gagasan dasar operasi militer selain perang dilandasi pertimbangan diperlukannya pendekatan baru yang kolaboratif dan lebih tangguh untuk menghadapi tantangan keamanan kontemporer, seperti terorisme, kejahatan transnasional, misalnya penyelundupan narkoba, senjata, dan manusia, pembajakan di laut, serta gerakan separatis. Berdasarkan latar belakang tersebut, membatasi fungsi militer hanya pada pertempuran konvensional melawan invasi asing atau perang antarnegara dianggap tidak rasional.

Kedua, revisi UU tentang TNI menetapkan perwira militer aktif dapat diangkat ke lima kementerian dan lembaga negara non-pertahanan, termasuk Badan Pengelola Perbatasan Nasional (BNPP), Badan Penanggulangan Bencana Nasional (BNPB), Badan Pemberantasan Terorisme Nasional (BNPT), Badan Keamanan Maritim (Bakamla), dan Kejaksaan Agung (Kejaksaan Agung);

Ketiga, wewenang TNI untuk merumuskan kebijakan dan strategi pertahanan nasional dilaksanakan dalam koordinasi dengan Kementerian Pertahanan. Hal ini berarti posisi markas besar militer menjadi relatif setara dengan Kementerian Pertahanan. Akibatnya, peningkatan otonomi TNI dalam urusan strategis kemungkinan akan mengurangi kontrol sipil terhadap masalah-masalah militer melalui kementerian tersebut.

Perubahan signifikan tersebut memang telah mengubah secara fundamental Undang-Undang No. 34/2004 tentang TNI. Undang-undang ini secara tegas melarang keterlibatan militer dalam politik, aktivitas bisnis, dan penunjukan politik lainnya. Menurut ketentuan undang-undang ini operasi militer selain perang terbagi menjadi 14 jenis operasi, termasuk kontra-pemberontakan, kontra-terorisme, bantuan bencana, keamanan perbatasan, penjaga perdamaian, dan bantuan militer kepada pemerintah daerah dan kepolisian. Undang-undang ini mewajibkan bahwa semua aktivitas operasi militer selain perang memerlukan keputusan politik negara dari presiden dan badan legislatif, yang berfungsi sebagai kerangka kerja untuk memastikan legalitas, kejelasan operasional, dan alokasi sumber daya sembari tetap mempertahankan pengawasan sipil.³¹⁴

Sejak pelantikan Presiden Prabowo, memang nampak upaya modernisasi pertahanan Indonesia telah meningkat secara signifikan. Pada Januari 2025, Kementerian Pertahanan Indonesia mengumumkan rencana untuk meningkatkan anggaran pertahanan, hampir menggandakannya dengan menetapkan target sebesar 1,5% dari produk domestik bruto (PDB) Indonesia, dibandingkan dengan 0,8% dari PDB dari anggaran sebelumnya yang dialokasikan untuk militer. Meskipun peningkatan anggaran tersebut tampaknya menandakan komitmen serius terhadap ekspansi militer. Indonesia tampaknya sedang gencar melakukan pembelian untuk mengisi kesenjangan pertahanan yang mendesak, namun kurang memiliki strategi terpadu untuk kohesi dan interoperabilitas militer. Upaya kerja sama militer dengan berbagai kekuatan, termasuk China, Amerika Serikat, Rusia, Korea Selatan, Jepang, dan Australia, berisiko

Gagasan ini selanjutnya dilembagakan melalui Undang-Undang Nomor 34 Tahun 2004 tentang TNI. Undang-undang tersebut menetapkan militer Indonesia memiliki dua fungsi utama, yaitu operasi militer dan Operasi Militer Selain Perang. Lihat, Haripin, *Civil-Military Relations in Indonesia*.

³¹⁴ Diandra Megaputri Mengko dan Aulia Fitri Rosadi, "Non-Institutionalised Civilian Control and Military Operations Other than War in Indonesia," dalam *Military Modernisation and Civil-Military Relations in Indonesia*, ed. Muhammad Haripin, Adhi Priamarizki, dan Leonard C. Sebastian (Singapore: Palgrave Macmillan, 2025).

melemahkan otonomi strategis Indonesia yang justru menempatkan Indonesia di tengah-tengah kepentingan geopolitik yang bersaing.³¹⁵

Upaya modernisasi TNI setidaknya dimulai pada 2009 di bawah skema Kekuatan Esensial Minimum (*Minimum Essential Force*). Skema ini dirancang untuk meningkatkan tiga sektor, yaitu kemampuan pengerahan, meningkatkan kekuatan serang, dan meningkatkan kemampuan operasi militer selain perang.³¹⁶

Modernisasi persenjataan di Indonesia merujuk pada Pedoman Kebijakan Pertahanan Umum yang ditetapkan berdasarkan Peraturan Presiden Republik Indonesia Nomor 111 Tahun 2025 Tentang Kebijakan Umum Pertahanan Negara Tahun 2025-2029. Regulasi ini mengidentifikasi ancaman hibrida terhadap Indonesia, meliputi serangan siber terintegrasi, serangan drone, penyalahgunaan kecerdasan artifisial, gangguan terhadap *Command Control, Communication Computers, Cyber-Defense, Combat System Intelligence, Surveillance and Reconnaissance* (C6ISR).³¹⁷ Pemanfaatan teknologi dwiguna dapat merujuk pada arah Kebijakan Pembinaan Kemampuan Teknologi dan Industri Pertahanan, mencakup:³¹⁸

1. Pembinaan kemampuan teknologi pertahanan diarahkan pada: (1) penguasaan teknologi kunci program prioritas yang memiliki rancang bangun, yaitu radar, satelit militer, alutsista nirawak (pesawat udara/kapal permukaan/kapal bawah air/kendaraan tanpa awak), dan/ atau penginderaan bawah permukaan air; (2)

³¹⁵ Kohesi dalam strategi pengadaan Indonesia masih terdapat kesenjangan yang tercermin dalam beragamnya negara yang menjadi tujuan pembelian senjata. Pada Juni 2025, Indonesia menyelesaikan akuisisi jet tempur TF KAAAN buatan Turkish Aerospace Industries. Berita ini muncul bersamaan dengan pengumuman potensi niat Indonesia untuk membeli jet tempur J-10 buatan China dan revisi kesepakatan Jakarta untuk pengadaan jet tempur KG-21 dengan Korea Selatan. Pembelian jet tempur Indonesia sebelumnya termasuk perjanjian dengan pabrikan AS Boeing untuk membeli 24 jet tempur F-15EX pada pertengahan 2023. Keragaman pemasok ini menciptakan tantangan interoperabilitas yang serius. penggunaan jet tempur yang beragam menunjukkan strategi reaktif yang dirancang untuk mengatasi kebutuhan militer mendesak dan tekanan geopolitik. Sifat akuisisi yang terfragmentasi ini sangat sedikit membantu pengoperasian peralatan, menciptakan masalah pemeliharaan, mengurangi pelatihan lintas sektor, dan melemahkan strategi militer jangka panjang Indonesia. Sebagai contoh, pelatihan silang antara platform jet tempur Turki, Tiongkok, Korea Selatan, dan Amerika akan sulit dikoordinasikan, yang secara efektif akan melemahkan pengaruh militer regional Indonesia. Akibatnya, Indonesia berisiko menciptakan militer yang terfragmentasi, berbeda dengan kekuatan tempur modern yang terkoordinasi. Lihat, Hugh Harsono, "Indonesia's Haphazard Military Acquisitions Risks Its Global Ambitions," *Small Wars Journal*, 29 September 2025, <https://smallwarsjournal.com/2025/09/29/indonesia-military-acquisitions-global-ambitions/>.

³¹⁶ Muhamad Haripin, Adhi Priamarizki, dan Leonard C. Sebastian, "Introduction: Reform Setbacks and Selective Emulation—The Path to Military Modernisation in Indonesia," dalam *Military Modernisation and Civil-Military Relations in Indonesia*, disunting oleh Muhamad Haripin, Adhi Priamarizki, dan Leonard C. Sebastian (Singapore: Palgrave Macmillan, 2025), 1–14.

³¹⁷ Lihat, Peraturan Presiden Republik Indonesia Nomor 111 Tahun 2025 Tentang Kebijakan Umum Pertahanan Negara Tahun 2025-2029.

³¹⁸ Peraturan Presiden Republik Indonesia Nomor 111 Tahun 2025 Tentang Kebijakan Umum Pertahanan Negara Tahun 2025-2029.

pembinaan kemampuan teknologi pendukung daya gempur, daya gerak, penginderaan, ataupun peperangan elektronik dan siber; (3) pembinaan kemampuan teknologi informasi dan komunikasi berbasis komputer dan jejaring dengan memperhatikan interoperabilitas sistem komando dan kendali; (4) pembinaan kemampuan sistem komunikasi, navigasi, penginderaan jarak jauh, dan intelijen berbasis satelit militer; (5) pemanfaatan Artificial Intelligence, himpunan data dalam jumlah besar (*big data*), *machine learning*, sistem otomasi, dan teknologi robot untuk kepentingan Pertahanan Negara;

2. Pembinaan kemampuan dukungan teknologi dan industri pertahanan diarahkan pada (3) penguatan industri bahan baku dan komponen strategis serta industri yang memanfaatkan teknologi dual-use (multiguna untuk penggunaan kepentingan sipil/militer) yang memiliki efek pengganda (*multiplier effect*) pada penguatan industri nasional.

Modernisasi persenjataan di Indonesia dikembangkan melalui gagasan kerja sama *triple helix*. Model ini dapat diharapkan akan menghasilkan dampak ekonomi yang lebih besar daripada sekadar memperoleh teknologi pertahanan melalui pengadaan. Lebih jauh, manfaat utamanya adalah potensi munculnya produk sampingan, yaitu teknologi militer yang digunakan kembali untuk keperluan sipil.³¹⁹ Dalam kaitan ini, modernisasi sering kali berfokus pada penggantian kemampuan yang ada dengan kemampuan yang lebih unggul dan mematikan, mencakup, antara lain, pengadaan senjata dan sistem jaringan baru. Modernisasi dikontekstualisasikan sebagai bagian dari perubahan yang lebih besar dan substansial, yaitu transformasi militer sehingga tidak hanya dikaitkan dengan domain piranti keras. Modernisasi seharusnya juga merambah pada domain piranti lunak atau prinsip dan doktrin mendasar yang menentukan prosedur dan pedoman penggunaan kekuatan militer.³²⁰

Namun demikian, perluasan penugasan tanggung jawab siber kepada militer secara signifikan memperluas peran angkatan bersenjata dalam pemerintahan sipil. Keterlibatan militer dalam keamanan siber tanpa strategi yang jelas untuk memandu kewenangannya ibarat menavigasi medan perang tanpa kompas. Keterlibatan militer dalam keamanan siber berpotensi memicu tindakan yang melanggar kebebasan sipil. Keamanan siber pada dasarnya bersinggungan dengan kehidupan sipil, mencakup isu-isu seperti privasi, kebebasan berekspresi, dan akses terhadap informasi. Pemberian peran kepada militer

³¹⁹ Priamarizki dan Caroline, *Prabowo's Defence Challenge*.

³²⁰ Priamarizki dan Caroline, *Prabowo's Defence Challenge*.

di bidang ini, tanpa pengawasan dan akuntabilitas yang ketat, berisiko mengikis prinsip-prinsip demokrasi dan HAM.³²¹

Pada saat bersamaan, RUU tentang Keamanan dan Ketahanan Siber (RUU KKS) yang telah ditetapkan sebagai prioritas legislasi nasional 2026, masih mengedepankan perlindungan keamanan negara ketimbang perlindungan warga negara berbasis HAM. Hal ini tampak dalam draf RUU KKS, khususnya Pasal 56 Ayat (1) Huruf d. Ketentuan dalam pasal tersebut membuka ruang pelibatan TNI dalam penanganan pidana siber. Perumusan ini menurut masyarakat sipil menjadi indikasi semakin menguatnya upaya militerisasi ruang siber. Draft RUU KKS juga menampilkan watak *draconian law*. Ini terlihat dalam penggunaan istilah makar di ruang siber yang tercantum dalam Pasal 61 Ayat (2) Huruf b. dengan ancaman pidana penjara sampai dengan 20 tahun penjara.³²²

Pendekatan yang berorientasi pada kepentingan pertahanan dan keamanan dalam pengaturan ruang siber berpotensi mengabaikan perlindungan kebebasan dan hak-hak dasar warga. Oleh karena itu, diperlukan pendekatan alternatif yang menempatkan perlindungan hak sebagai bagian dari tujuan keamanan siber. Salah satu pendekatan tersebut dikemukakan oleh Ronald J. Deibert, yang mengkritik pendekatan keamanan siber yang berpusat pada keamanan nasional dan mengutamakan kedaulatan teritorial. Sebagai alternatif, ia menawarkan pendekatan yang berlandaskan keamanan manusia (*human security*), yang menempatkan individu sebagai objek utama keamanan. Dalam pendekatan ini, jaringan digital dipandang sebagai fondasi penting bagi pelaksanaan HAM, termasuk akses terhadap informasi, kebebasan berpikir, dan kebebasan berserikat. Pendekatan ini juga menekankan pentingnya pengawasan independen untuk memastikan keamanan jaringan tetap sejalan dengan perlindungan HAM. Pendekatan yang berpusat pada manusia semestinya menjadi paradigma dan logika dalam menyusun RUU KKS yang masih kental nuansa berpusat pada keamanan nasional. Pendekatan ini masih berangkat dari teori realis politik dunia bahwa negara-negara saling bersaing demi kelangsungan hidup dan keunggulan relatif. Oleh karena itu, ancaman utama keamanan siber dipahami sebagai ancaman yang berdampak pada negara berdaulat, seperti kerusakan infrastruktur kritis di dalam wilayah yurisdiksi mereka.³²³

Sementara itu, adopsi teknologi militer baru tidak terjadi dalam ruang hampa, namun dipengaruhi faktor-faktor domestik, seperti dinamika politik, sosial, ekonomi, dan budaya.

³²¹ Gatra Priyandita dan Christian Guntur Lebang, "Indonesia's Cyber Soldiers: Armed without a Compass," *The Strategist*, 11 April 2025, <https://www.aspistrategist.org.au/indonesias-cyber-soldiers-armed-without-a-compass/>.

³²² Machradin Wahyudi Ritonga, "Dinilai Cederai Demokrasi, Wewenang TNI dalam RUU Keamanan dan Ketahanan Siber Jadi Sorotan," *Kompas.id*, 4 Oktober 2025, <https://www.kompas.id/artikel/dinilai-cederai-demokrasi-wewenang-tni-dalam-ruu-keamanan-dan-ketahanan-siber-jadi-sorotan>.

³²³ Ronald J. Deibert, "Toward a Human-Centric Approach to Cybersecurity," *Ethics & International Affairs* 32, no. 4 (2018): 411–424, <https://doi.org/10.1017/S0892679418000618>.

Emily O. Goldman dan Andrew L. Ross menekankan faktor situasional dan pilihan kebijakan sebagai faktor penting dalam menentukan jalur adopsi negara. Faktor situasional terdiri dari geografi, kapasitas sumber daya ekonomi, dan lingkungan sosial, politik, budaya, dan organisasi. Sementara itu, pilihan kebijakan menyiratkan komitmen pemerintah terhadap arah kebijakan tertentu.³²⁴

Dalam pengertian ini, modernisasi militer sering dibentuk oleh:³²⁵

1. Persepsi pembuat kebijakan terhadap potensi musuh atau ancaman keamanan;
2. Pemahaman politik dan geografis yang memengaruhi para pembuat kebijakan dan penduduk dalam mendefinisikan wilayah nasional mereka dan keterbatasannya;
3. Pandangan dan aspirasi tentang kemampuan masa depan yang harus dikembangkan untuk mencegah dan mengalahkan musuh potensial.

Selain pertimbangan domestik, modernisasi militer juga dipengaruhi oleh dinamika politik yang membentuk hubungan antara militer dan pemerintahan sipil. Dengan demikian, modernisasi militer tidak hanya ditentukan oleh kebutuhan dan pertimbangan profesional militer, tetapi juga oleh dinamika hubungan sipil-militer. Dalam konteks ini, politisasi militer dan intervensi sipil dapat menjadi faktor yang memengaruhi, bahkan menghambat, proses modernisasi militer. Namun politisasi militer juga dapat terjadi karena pelanggaran yang disengaja oleh militer terhadap urusan sipil/non-pertahanan.

Secara historis militer di Indonesia merupakan aktor politik yang aktif dan memainkan peran penting dalam pembuatan kebijakan dalam negeri dan luar negeri. Dengan dalih keamanan nasional, misalnya, militer mengambil inisiatif untuk memperluas perannya dalam berbagai misi sosial-ekonomi (non-pertahanan) dan penegakan hukum. Peran militer, khususnya kewenangan operasi militer selain perang, termasuk modernisasi militer akan mewarnai hubungan sipil-militer di Indonesia, khususnya campur tangan politik militer Indonesia baru-baru ini. Dalam kaitan ini terdapat dua argumen dalam menjelaskan fenomena hubungan sipil dan militer. *Pertama*, perluasan kehadiran militer di luar urusan pertahanan didorong oleh keinginan militer untuk melindungi kepentingan korporatnya, terutama tingkat supremasi dalam politik. Militer berupaya mempertahankan kehadirannya dalam berbagai kegiatan, seperti tugas-tugas sipil dan kontra-terorisme. Upaya-upaya di luar urusan pertahanan tersebut memungkinkan pelestarian pengaruh politiknya. *Kedua*, keterlibatan politik sebagai produk dinamika organisasi yang difasilitasi oleh transaksionalisme politik dengan pihak sipil.³²⁶

³²⁴ Haripin, Priamarizki, dan Sebastian, "Introduction: Reform Setbacks and Selective Emulation."

³²⁵ Haripin, Priamarizki, dan Sebastian, "Introduction: Reform Setbacks and Selective Emulation."

³²⁶ Haripin, Priamarizki, dan Sebastian, "Introduction: Reform Setbacks and Selective Emulation."

Militerisasi tidak hanya berlangsung dalam ranah pertahanan dan konflik bersenjata, tetapi juga merambah kehidupan sehari-hari masyarakat sipil. Paul Virilio menggunakan konsep *pure war* (perang murni) untuk menggambarkan kondisi ketika logika perang dan persiapan militer terus berlangsung, bahkan pada masa damai, sehingga batas antara ranah sipil dan militer semakin kabur.³²⁷ Pemikiran ini dapat dikaitkan dengan gagasan Stephen Graham tentang *militarization of everyday life* (militerisasi kehidupan sehari-hari), yang menjelaskan bagaimana teknologi, praktik, dan logika militer semakin meresap ke dalam kehidupan sipil. Graham, misalnya, menunjukkan bagaimana militerisasi berlangsung dalam tata kelola perkotaan melalui penggunaan teknologi pelacakan, pemilahan, dan pembuatan profil penduduk, termasuk perangkat lunak pengenalan wajah. Ia juga menyoroti kecenderungan memandang kota sebagai ruang yang mengandung ancaman, yang turut mendorong perluasan praktik pengawasan serta penggunaan perlengkapan taktis dan persenjataan berdaya tinggi oleh kepolisian. Perkembangan teknologi digital dapat memperluas praktik-praktik tersebut, terutama melalui peningkatan kapasitas pengawasan dan pengumpulan data terhadap penduduk.³²⁸

Meluasnya militerisasi ke ranah sipil dapat memperkuat kapasitas represif rezim otoriter. Hal ini terjadi ketika teknologi persenjataan modern, yang diperoleh dari luar negeri, semakin banyak digunakan oleh aparat keamanan untuk mengendalikan masyarakat. Persenjataan yang lebih cepat dan akurat memungkinkan aparat menekan protes dan kerusuhan secara lebih efektif dengan biaya yang lebih rendah. Akses ke teknologi militer modern secara substansial mengurangi kemungkinan demokratisasi rezim otoriter. Hal ini berarti senjata modern memainkan peran kunci dalam menekan gerakan demokrasi. Singkatnya, semakin banyak demonstran yang mengalami tindakan represif oleh suatu rezim dengan menggunakan sumber daya sesedikit mungkin dan pada saat bersamaan penggunaan teknologi tersebut semakin memperkuat rezim tersebut.³²⁹ Keberhasilan gerakan pro-demokrasi sangat bergantung pada kemampuan atau ketidakmampuan penguasa untuk mempergunakan instrumen kekerasan terhadap para pengunjuk rasa dan kemampuan ini bergantung pada teknologi persenjataan.

³²⁷ Setelah Perang Dunia II, menurut Paul Virilio ekonomi dan masyarakat Barat ditata ulang secara permanen untuk mendukung kekuatan militer. Fokus beralih dari taktik medan perang ke strategi yang lebih luas, yang bertujuan merestrukturisasi masyarakat industri agar mampu memproduksi roket, rudal, dan persenjataan lainnya secara cepat. Dalam konteks kemajuan teknologi digital belakangan ini, teknologi komputasi, algoritmik, dan penginderaan menjadi titik tuju masyarakat industri. Lihat, Ben Egliston dan Marcus Carter, "The Dangerous Fantasy of Cybernetic Cops," *The MIT Press Reader*, 16 September 2024, <https://thereader.mitpress.mit.edu/the-dangerous-fantasy-of-cybernetic-cops/>.

³²⁸ Egliston dan Carter, "The Dangerous Fantasy of Cybernetic Cops."

³²⁹ Asger Mose Wingender dan Søren Bang, "Modern Arms Technologies Help Autocratic Rulers Stay in Power," *University of Copenhagen*, 25 Januari 2023, https://news.ku.dk/all_news/2023/01/modern-arms-technologies-help-autocratic-rulers-stay-in-power.

Oleh karena teknologi persenjataan modern kini telah menjadi jauh lebih efektif dan lebih murah, maka dengan sumber daya yang tersedia bagi rezim otokratis saat ini, bahkan negara termiskin di dunia memiliki akses ke teknologi persenjataan canggih yang baru berusia beberapa dekade. Senjata lebih hemat biaya, dan teknologi telah menyebar ke negara-negara miskin, memberi penguasa otoriter akses ke sarana represi yang kuat.³³⁰

Sementara itu, pemerintahan otoriter di seluruh dunia semakin memanfaatkan kekuasaannya untuk menjangkau operator jaringan, penerapan kerangka kebijakan dan hukum yang ketat, serta mendapatkan teknologi pengawasan dan sensor untuk meningkatkan kemampuan represi digital mereka.³³¹ Asger Mose Wingender dan Jacob Gerner Hariri melihat fenomena ini bukan sebagai sesuatu yang sepenuhnya baru. Secara historis, perkembangan teknologi militer berjalan beriringan dengan kemajuan ekonomi dan teknologi lainnya. Di Eropa Barat, kebutuhan negara untuk membiayai perang mendorong pemungutan pajak dari masyarakat. Ketergantungan negara pada pajak tersebut kemudian memperkuat posisi tawar masyarakat dalam menuntut hak politik, termasuk hak untuk memilih. Tuntutan tersebut turut berkontribusi terhadap proses demokratisasi. Namun kini tekanan pada rezim otokratis lebih rendah. Senjata kini lebih murah dan teknologi telah menyebar ke negara-negara miskin. Situasi ini memberi penguasa otoriter akses ke sarana represi. Akibatnya, ketidakseimbangan muncul antara perkembangan teknologi militer dan perkembangan ekonomi yang menghambat demokratisasi. Perkembangan ekonomi memang dapat memperkuat tuntutan masyarakat terhadap demokrasi. Namun, pada saat yang sama, akses rezim otokratis terhadap teknologi persenjataan modern meningkatkan kemampuan negara untuk menekan gerakan pro-demokrasi. Perkembangan yang tidak seimbang antara modernisasi ekonomi dan kemajuan teknologi persenjataan tersebut dapat memperkuat posisi negara terhadap masyarakat, sehingga menghambat proses demokratisasi.³³²

Teknologi digital telah memberikan pemerintah otokratis dan illiberal kemampuan yang belum pernah ada sebelumnya untuk mempertahankan kekuasaan melalui penggunaan teknologi surveilans, propaganda, dan disinformasi. Beberapa teknologi mengakibatkan penindasan dan kontrol yang jauh lebih meluas, efisien, dan halus. Otoritarianisme digital mengambil banyak bentuk, seperti pelecehan daring, disinformasi, pemadaman internet, serangan siber, dan surveilans terarah menggunakan media sosial, kecerdasan artifisial, dan piranti lunak pengenalan wajah. Beberapa negara, khususnya negara adidaya ekonomi dan teknologi tentu lebih canggih daripada taktik para pemimpin dari negara-negara berkembang. Namun demikian teknologi yang lebih rendah bukan berarti ancaman yang

³³⁰ Wingender dan Bang, "Modern Arms Technologies Help Autocratic Rulers Stay in Power."

³³¹ Irene Poetranto, "The Architecture of Digital Repression: Internet Service Providers Can Facilitate Internet Access but Also Draconian Control," *Carnegie Endowment for International Peace*, 10 Maret 2026, <https://carnegieendowment.org/research/2026/03/the-architecture-of-digital-repression>.

³³² Wingender dan Bang, "Modern Arms Technologies Help Autocratic Rulers Stay in Power."

ditimbulkannya juga berkurang. Pemerintah dengan sumber daya politik, teknologi, dan ekonomi yang kurang memadai tetap mampu mengikis demokrasi dan HAM.

Selain itu, penting untuk memahami bahwa unsur-unsur otoritarianisme digital dapat dan memang ada di negara-negara demokrasi liberal, seperti Kanada dan Amerika Serikat. Faktanya, penurunan demokrasi global dalam 15 tahun terakhir bertepatan dengan munculnya teknologi baru untuk pengumpulan informasi, komunikasi, dan surveilans. Para pemimpin dan pemerintah otoriter telah belajar memanfaatkan digitalisasi. Para pemimpin tersebut menyadari bahwa kelangsungan rezim mereka dapat bergantung pada kemampuan mereka untuk memanfaatkan teknologi digital sebagai instrumen pengendalian dan represi terhadap warga negara. Otoritarianisme telah bertransformasi seiring dengan perkembangan teknologi digital. Transformasi ini ditandai oleh pemanfaatan teknologi informasi digital oleh rezim otoriter untuk mengawasi, menindas, dan memanipulasi penduduk, baik di dalam negeri maupun di luar negeri.³³³

Rezim otoriter, terlepas dari tampilan luarnya yang kadang tampak demokratis, pada akhirnya bergantung pada kekuatan dan kapasitas represif. Meskipun rezim otoriter mungkin membangun lembaga-lembaga yang secara lahiriah meniru kerangka kerja demokratis, rezim-rezim tersebut sebenarnya lebih berkepentingan untuk melanggengkan kekuasaan mereka melalui paksaan, penindasan, dan penekanan perbedaan pendapat.³³⁴ Kapasitas represif merupakan ciri utama rezim otoriter. Kapasitas ini mencerminkan kemampuan negara menggunakan kekuatan koersif untuk mempertahankan kekuasaan dan mengendalikan masyarakat. Hal tersebut dapat dilihat dari kemampuan rezim menekan protes dan membatasi perbedaan pendapat, serta pengaruhnya terhadap peluang demokratisasi. Kapasitas represif juga berkaitan dengan sumber daya yang dialokasikan untuk sektor keamanan, termasuk anggaran dan jumlah personel keamanan.³³⁵

Tiberiu Dragu dan Yonatan Lupu menunjukkan perkembangan teknologi justru memperkuat kontrol rezim otoriter. Inovasi teknologi mendorong peningkatan tingkat pelanggaran untuk mencegah kelompok oposisi melakukan mobilisasi dan meningkatkan kemungkinan otoritarian berhasil mencegah mobilisasi

³³³Marie Lamensch, "Authoritarianism Has Been Reinvented for the Digital Age," *Centre for International Governance Innovation*, 9 Juli 2021, <https://www.cigionline.org/articles/authoritarianism-has-been-reinvented-for-the-digital-age/>.

³³⁴Tiberiu Dragu dan Germán Gieczewski, "Strength in Numbers? State Capacity, Military Power and Repression in Authoritarian Regimes," working paper (New York: Department of Politics, New York University; Princeton: Department of Politics, Princeton University, Maret 2024).

³³⁵Namun demikian analisis proksi untuk menelusuri represifitas suatu rezim mungkin merupakan indikator yang tidak akurat dari kapasitas represif atau kekuatan militer ketika terdapat korupsi yang signifikan atau masalah keagenan lainnya dalam pasukan keamanan. Lihat, Dragu dan Gieczewski, "Strength in Numbers?"

tersebut. Hasil ini memiliki implikasi luas bagi rezim HAM, upaya demokratisasi, dan upaya menurunkan pelanggaran HAM yang disertai penyalahgunaan.³³⁶

Lebih jauh, Dragu dan Lupu mengemukakan dua hal penting dalam memahami dampak teknologi digital terhadap HAM di bawah rezim otoriter.³³⁷ Pertama, teknologi digital dapat memperkuat penindasan preventif, yaitu upaya pemerintah untuk mencegah kelompok oposisi memobilisasi dan mengorganisasi perlawanan. Teknologi memungkinkan pemerintah mengidentifikasi dan memantau calon oposisi sebelum mereka menjadi ancaman nyata. Penindasan preventif dapat berbentuk pelanggaran HAM nonfisik, seperti surveilans massal dan sensor, tetapi juga dapat melibatkan kekerasan. Berbeda dengan penindasan reaktif yang dilakukan untuk merespons perlawanan yang telah berlangsung dan dapat berujung pada kekejaman massal, penindasan preventif bertujuan mencegah mobilisasi oposisi sejak awal.

Kedua, dampak teknologi terhadap HAM perlu dipahami melalui interaksi strategis antara pemerintah otoriter dan kelompok oposisi. Teknologi digital dapat meningkatkan kemampuan kedua pihak, baik untuk melakukan penindasan maupun untuk memobilisasi perlawanan. Namun, inovasi teknologi dapat memperbesar kemampuan pemerintah mencegah mobilisasi oposisi sekaligus meningkatkan pelanggaran HAM yang dilakukan dalam proses tersebut.

Dengan demikian, perubahan dalam teknologi digital memiliki dampak penting terhadap HAM. Teknologi digital memberdayakan masyarakat sipil dengan menurunkan biaya mobilisasi sehingga memfasilitasi pengorganisasian gerakan protes dan bentuk-bentuk pembangkangan yang dimobilisasi lainnya. Upaya memobilisasi pembangkangan publik mahal dan keberhasilan gerakan aktivis dan kelompok oposisi sering kali sebagian bergantung pada upaya untuk mengurangi biaya tersebut. Peningkatan adopsi internet berkorelasi dengan transisi menuju demokrasi dan tingkat demokrasi yang lebih tinggi. Hal ini menunjukkan adanya efek mobilisasi teknologi (*mobilization effect of technology*) untuk mendukung klaim HAM.³³⁸

Sebagai contoh, pada 2016, Partai Komunis China mengarahkan salah satu kontraktor pertahanan milik negara terbesar, China Electronics Technology Group, untuk mengembangkan perangkat lunak yang dapat mengumpulkan data tentang pekerjaan, hobi, transaksi keuangan, dan kebiasaan konsumsi warga China. Permintaan itu juga mencakup perangkat lunak untuk menganalisis perilaku daring warga serta alat berbasis kecerdasan buatan untuk mengidentifikasi wajah orang yang terekam kamera keamanan. Sistem pengawasan baru ini menambah kumpulan data yang sudah besar yang telah dikumpulkan pemerintah China sebelumnya. Memiliki data setiap warga negara,

³³⁶ Dragu dan Lupu, "Digital Authoritarianism and the Future of Human Rights."

³³⁷ Dragu dan Lupu, "Digital Authoritarianism and the Future of Human Rights."

³³⁸ Dragu dan Lupu, "Digital Authoritarianism and the Future of Human Rights."

memungkinkan pemerintah menandai mereka yang berpotensi menjadi ancaman. Meskipun tujuan yang dinyatakan dari kebijakan baru ini adalah untuk memerangi terorisme, namun dikhawatirkan tujuan sebenarnya penggunaan piranti itu untuk membantu membungkam oposisi sejak tahap awal, mencegah peristiwa seperti Lapangan Tiananmen dan lainnya tidak terjadi. Tidak mengherankan bahwa Partai Komunis China memanfaatkan perkembangan terbaru dalam teknologi surveilans untuk memperkuat upaya represi preventifnya. Dalam pengertian ini, represi preventif bersifat *ex ante*, dilakukan sebelum protes atau demonstrasi terjadi. Ini berbeda dengan represi perbaikan yang terjadi *ex post*, setelah represi pencegahan gagal dan protes publik terwujud.³³⁹

Situasi ini menunjukkan paradoks teknologi baru yang berdampak pada (1) kemampuan pemerintah untuk secara preventif membungkam upaya kelompok oposisi dalam memobilisasi protes publik dan (2) kemampuan kelompok oposisi untuk memobilisasi perbedaan pendapat. Teknologi tertentu yang dapat membantu warga berorganisasi juga dapat digunakan pemerintah otoriter membungkam kelompok oposisi bahwa sejak tahap awal; sebelum mereka benar-benar menentang pemerintah yang otoriter.³⁴⁰

Tidak ada rezim otoriter yang ingin menghadapi situasi di mana perbedaan pendapat telah tumbuh cukup kuat untuk memerlukan intervensi militer skala besar guna mempertahankan kekuasaan. Para penguasa enggan melakukan perbaikan akibat penindasan yang dilakukan oleh militer setidaknya karena dua alasan.

Pertama, dalam skenario akhir seperti itu, rezim harus bergantung pada kepatuhan warga yang bisa mahal dan tidak efektif. Militer tidak terlatih, tidak dilengkapi secara khusus, dan tidak termotivasi untuk terlibat dalam represi domestik, sehingga menggunakan mereka untuk membungkam protes biasanya menjadi upaya terakhir.

Kedua, meminta dan mengandalkan militer melibatkan risiko politik yang cukup besar dalam hal kelangsungan rezim, baik karena militer mungkin menolak untuk mematuhi perintah represi atau karena militer dapat mengeksploitasi kerentanan rezim untuk menggulingkannya.³⁴¹

William J. Dobson mengamati bahwa rezim otoriter saat ini telah menggantikan bentuk-bentuk kekerasan brutal dan pembunuhan massal dengan metode kontrol dan paksaan yang halus. Rezim otoriter telah menyempurnakan penggunaan rasa takut dan intimidasi untuk mempertahankan cengkeraman kekuasaan mereka dan telah belajar untuk mengandalkan propaganda, sensor, dan kooptasi sebagai pengganti represi skala besar

³³⁹ Tiberiu Dragu dan Adam Przeworski, "Preventive Repression: Two Types of Moral Hazard," *American Political Science Review* 113, no. 1 (2019): 77–87, <https://doi.org/10.1017/S0003055418000552>.

³⁴⁰ Dragu dan Lupu, "Digital Authoritarianism and the Future of Human Rights."

³⁴¹ Dragu dan Lupu, "Digital Authoritarianism and the Future of Human Rights."

terhadap perbedaan pendapat publik. Meskipun penting, represi hanyalah salah satu instrumen yang digunakan penguasa otoriter untuk mempertahankan kekuasaan mereka. Selain represi, para otokrat dapat: (1) merangkul beberapa calon lawan; (2) terlibat dalam propaganda; (3) merekayasa pemilihan untuk melegitimasi kekuasaan atau menciptakan tiruan masyarakat sipil dengan mendirikan organisasi masyarakat sipil yang dioperasikan pemerintah. Represi paling efektif ketika tidak terlihat, ketika rezim bertahan tanpa harus memukuli, menembakkan gas air mata, atau membunuh warganya.³⁴²

Akibatnya, rezim otoriter terutama menggunakan dan bergantung pada represi preventif, yang secara rutin dilakukan oleh badan-badan keamanan khusus, biasanya menggunakan polisi rahasia, yang terkadang disebut sebagai badan intelijen. Polisi rahasia mempekerjakan mata-mata profesional dan informan paruh waktu untuk mendeteksi potensi oposisi dengan mengandalkan informan, mencegat komunikasi, menanam alat penyadap, dan sejenisnya. Tindakan ini dapat juga mencakup eliminasi fisik, pemenjaraan, sanksi ekonomi, larangan bepergian, intimidasi, pemerasan, pelecehan psikologis dan fisik, dan sejenisnya. Pencegahan juga dapat mencakup sensor, penyebaran informasi dan rumor palsu, dan distorsi komunikasi di antara kelompok oposisi.³⁴³

Pemanfaatan polisi rahasia (badan intelijen) dimungkinkan karena kekuasaan politik memberikan penguasa, baik individu maupun kolektif, akses ke beberapa sumber daya. Untuk melindungi kekuasaan ini, penguasa mempekerjakan badan-badan keamanan. Sebagai imbalannya, untuk menjalankan tugasnya, badan keamanan membutuhkan sarana yang diperlukan, baik itu bangunan, kendaraan, senjata, peralatan mata-mata, dana untuk membayar informan sehingga penguasa harus menyediakan sumber daya operasional selain membayar gaji agen keamanan.³⁴⁴

Berdasarkan anggaran keamanan ini, agen keamanan harus membuat keputusan mengenai alokasi dana, menentukan berapa banyak yang akan dialokasikan untuk perlindungan aktual dan berapa bagian yang akan dialokasikan untuk konsumsi pribadi. Proporsi sumber daya yang digunakan agen untuk keperluan pribadi menunjukkan prevalensi korupsi dan masalah keagenan lainnya yang dapat memengaruhi hubungan antara penguasa dan agen keamanannya. Kehadiran korupsi menunjukkan bahwa tidak semua sumber daya anggaran akan dialokasikan untuk langkah-langkah keamanan aktual. Pengeluaran anggaran yang lebih tinggi setidaknya berkorelasi dengan kapasitas represif yang lebih tinggi. Sebaliknya, ketika tingkat korupsi lebih tinggi, terdapat hubungan negatif antara pengeluaran anggaran dan kapasitas represif aktual. Dalam kasus tingkat korupsi yang lebih tinggi, maka menyebabkan peningkatan pengeluaran

³⁴² Dragu dan Przeworski, "Preventive Repression."

³⁴³ Dragu dan Przeworski, "Preventive Repression."

³⁴⁴ Dragu dan Przeworski, "Preventive Repression."

anggaran. Secara paradoks, peningkatan dana ini tidak dialokasikan secara proporsional untuk meningkatkan perlindungan aktual.³⁴⁵

Peluang korupsi melemahkan rezim otoriter dengan mendistorsi insentif badan-badan keamanan yang bertugas mencegah oposisi domestik. Aparat keamanan dapat mengalihkan upaya dan sumber daya untuk meningkatkan konsumsi mereka dengan terlibat dalam kegiatan mencari keuntungan yang tidak mengurangi keuntungan para pimpinan mereka. Agen polisi rahasia dapat terlibat dalam korupsi, menambah pengeluaran mereka, menjual jasa mereka kepada pihak swasta, atau berinvestasi dalam usaha ekonomi swasta.³⁴⁶

Selain moral hazard korupsi, rezim otoriter juga berisiko menghadapi moral hazard politik. Hal ini terjadi ketika agen (badan keamanan) dapat menggunakan pengaruh politik untuk meningkatkan keuntungan mereka dengan mengurangi keuntungan penguasa. Masalah risiko politik ini, diilustrasikan oleh fakta bahwa di hampir setiap rezim otokratis, hubungan antara penguasa dan agen keamanan mereka selalu tegang. Lembaga keamanan yang kuat merupakan pedang bermata dua bagi elite politik. Lembaga tersebut dapat lebih efektif dalam melindungi rezim, tetapi juga menciptakan masalah moral hazard karena kendali *de facto*-nya atas instrumen-instrumen kekerasan. Lembaga keamanan dapat menggunakan alat dan sumber daya mereka untuk terlibat dalam pertempuran politik di dalam rezim dan untuk meningkatkan kekuasaan politik mereka dan keuntungan yang terkait dengan kekuasaan itu terhadap para pemimpin politik mereka.³⁴⁷

Laporan Tempo dan sejumlah media serta aktivis HAM telah menemukan bahwa pemerintah Indonesia telah membeli sejumlah besar perangkat surveilans dari luar negeri antara tahun 2017 dan 2023. Ratusan perangkat ini, senilai puluhan triliun rupiah, diyakini telah diimpor secara diam-diam oleh sejumlah organisasi yang menggunakan perantara negara. Di Indonesia, para pembeli ini termasuk Kepolisian RI, Badan Intelijen Negara, dan Badan Siber dan Sandi Nasional. Penggunaan perangkat surveilans sering kali dilandasi argumentasi membantu penegak hukum mengungkap kejahatan seperti korupsi dan terorisme. Namun, tanpa kontrol yang ketat, piranti surveilans ini dapat dengan mudah disalahgunakan untuk memantau pergerakan kelompok-kelompok yang mengkritik pemerintah. Pembelian diam-diam dari negara-negara yang tidak memiliki hubungan diplomatik dengan Indonesia, seperti Israel mengindikasikan upaya menghindari pengawasan publik dan kendali yudisial.

Pembelian piranti surveilans pengawasan secara diam-diam merupakan ancaman bagi demokrasi dan hak privasi masyarakat. Hal ini juga rentan terhadap penggelapan dan penyalahgunaan. Pengadaan peralatan pengawasan secara rahasia tidak hanya

³⁴⁵ Dragu dan Gieczewski, "Strength in Numbers?"

³⁴⁶ Dragu dan Przeworski, "Preventive Repression."

³⁴⁷ Dragu dan Przeworski, "Preventive Repression."

meningkatkan risiko korupsi tetapi juga membuka pintu bagi penyalahgunaan kekuasaan. Tanpa sistem akuntabilitas yang kuat, teknologi ini dapat dengan mudah digunakan untuk memata-matai atau menekan suara-suara kritis yang penting bagi kesehatan demokrasi.³⁴⁸

Selain itu, piranti surveilans berpotensi digunakan oleh TNI untuk menunjang perluasan peran TNI dalam menanggulangi ancaman siber, termasuk keterlibatan TNI sebagai penyelidik keamanan dan pertahanan siber yang akan diatur melalui Undang-Undang Keamanan dan Ketahanan Siber. Penggunaan piranti menunjukkan kecenderungan Pemerintah Indonesia menggunakan model represi preventif untuk menjaga mereka dari ancaman siber. Kementerian Pertahanan pernah membeli perlengkapan intelijen canggih dari Inggris seharga £ 4,21 juta atau setara Rp71,35 miliar, bernama Finfisher. Piranti ini efektif untuk menyadap aktivitas seseorang melalui internet dan telepon seluler (ponsel). Menurut dokumen laporan United Kingdom (UK) Export Finance periode 2012-2013, terdapat transaksi jual-beli peralatan intelijen antara pemerintah Indonesia yang diwakili Menteri Pertahanan Purnomo Yusgiantoro dengan Gamma TSE Ltd. Memang, dokumen itu tidak merinci alat apa saja yang ada dalam transaksi jual-beli tersebut.³⁴⁹ Piranti *spyware* FinSpy milik FinFisher sebelumnya telah dikaitkan dengan Indonesia. Pada Maret 2013, Citizen Lab menerbitkan laporan berdasarkan pengukuran pemindaian internet yang mengidentifikasi server pelanggan FinSpy yang dihosting di Indonesia. Publikasi lanjutan tahun 2015 berdasarkan pemindaian internet oleh Citizen Lab mengaitkan server FinFisher dengan Badan Sandi Negara yang pada tahun 2017 berganti nama menjadi Badan Siber dan Sandi Negara.³⁵⁰

Upaya surveilans media sosial juga dapat ditelusuri saat terjadi pandemi COVID 19. Markas Besar Kepolisian Negara Republik Indonesia (Mabes Polri) secara resmi telah menerbitkan surat telegram yang memuat pedoman penegakan hukum dalam menangani tindak pidana di tengah wabah virus corona (COVID-19). Polri telah meningkatkan pemantauan media sosial sebagai upaya mencegah penyebaran informasi palsu serta komentar yang mencemarkan nama baik Presiden dan pejabat pemerintah selama wabah COVID-19 berlangsung.³⁵¹ Kemudian paket pengadaan sistem monitoring

³⁴⁸ Tempo Editorial, "The Dark Threat of Surveillance Equipment," *Tempo.co*, 9 Mei 2024, <https://en.tempo.co/read/1865183/the-dark-threat-of-surveillance-equipment>.

³⁴⁹ Kontan.co.id, "Kemhan Beli Penyadap Canggih Rp 71,35 Miliar," <https://nasional.kontan.co.id/news/kemhan-beli-penyadap-canggih-rp-7135-miliar>.

³⁵⁰ Amnesty International, *A Web of Surveillance*.

³⁵¹ Surat telegram resmi tersebut ditandatangani oleh Kepala Badan Reserse Kriminal (Kabareskrim), Komisaris Jenderal Listyo Sigit Prabowo, pada tanggal 4 April 2020. Tiga jenis pelanggaran utama yang akan dipantau oleh patroli siber kepolisian meliputi penyebaran hoaks terkait virus corona, ujaran yang memojokkan pemerintah dan Presiden, serta penipuan daring terkait penjualan perlengkapan kesehatan. Lihat, Dimas Kuncoro, "Coronavirus Crackdown Aimed at Anti-President Smears, Hoaxes," *Tempo.co*, 6 April 2020, <https://en.tempo.co/read/1328272/coronavirus-crackdown-aimed-at-anti-president-smears-hoaxes>.

media sosial senilai Rp49,2 miliar oleh Kementerian Pertahanan tahun anggaran 2026 melalui penunjukan langsung dengan satuan kerja (satker) Mabes TNI Angkatan Darat, memperlihatkan kecenderungan tersebut.³⁵²

Peningkatan penggunaan perangkat *spyware* komersial dan jenis teknologi surveilans lainnya oleh pemerintah menimbulkan ancaman serius terhadap HAM di seluruh dunia. Kepolisian dan dinas intelijen di banyak negara menggunakan teknologi tersebut untuk menargetkan aktivis, jurnalis, pekerja kemanusiaan, akademisi, dan suara-suara kritis lainnya, yang merusak lembaga-lembaga demokrasi, mempersempit ruang sipil, melanggar privasi dan hak-hak korban lainnya, dan dalam banyak kasus, mengancam keamanan fisik mereka.³⁵³ Piranti *spyware* mengancam hak privasi individu yang menjadi target. Meskipun gangguan tertentu terhadap privasi diperbolehkan, hukum HAM internasional menetapkan bahwa setiap pembatasan hak yang sah harus diatur oleh hukum, untuk mencapai tujuan yang sah dan proporsional, artinya tidak lebih dari yang diperlukan dalam masyarakat demokratis.³⁵⁴ Penggunaan teknologi *spyware* dalam batas-batas koridor tujuan yang sah, proporsionalitas masih diperdebatkan, mengingat sifatnya yang mengganggu karena infeksi *spyware* dapat memberikan akses dan membuka, antara lain, data komunikasi, geolokasi, kamera, dan mikrofon pada perangkat yang ditargetkan. Hal ini memungkinkan akses tidak hanya secara *real-time* tetapi juga retrospektif ke data individu yang ditargetkan serta individu-individu lain yang berhubungan dengan mereka, mengubah ponsel menjadi apa yang disebut oleh Kantor Komisioner Tinggi PBB untuk HAM (OHCHR) sebagai piranti surveilans 24 jam. Bagi banyak target *spyware*, pelanggaran terhadap esensi hak privasi mereka tampak jelas. Hal ini dapat diartikan gangguan tersebut sangat parah sehingga individu tersebut kehilangan hak tersebut.

Pada Mei 2019, David Kaye, Pelapor Khusus PBB tentang kebebasan berpendapat dan berekspresi, menyatakan keprihatinan serius tentang status ekspor surveilans. Dalam laporan tersebut, Pelapor Khusus PBB menjelaskan bahwa surveilans digital bukan lagi hak prerogatif negara-negara yang memiliki sumber daya internal untuk melakukan surveilans massal dan terarah. Pelapor Khusus menekankan bahwa negara-negara yang membeli teknologi surveilans harus mengambil langkah-langkah untuk memastikan bahwa penggunaannya sesuai dengan hukum HAM internasional, termasuk memperkuat hukum nasional untuk membatasi surveilans, menciptakan mekanisme publik untuk

³⁵² Kompas.id, "Anggaran Rp 492 Miliar untuk Monitoring Medsos TNI AD Dipertanyakan Publik," 28 April 2026, <https://www.kompas.id/artikel/anggaran-rp-492-miliar-untuk-monitoring-medsos-tni-ad-dipertanyakan-publik>.

³⁵³ Human Rights Watch, *Looking the Other Way: EU Failure to Prevent Surveillance Exports to Rights Violators* (12 Mei 2026), <https://www.hrw.org/report/2026/05/12/looking-the-other-way/eu-failure-to-prevent-surveillance-exports-to-rights>.

³⁵⁴ Riecke, "Unmasking the Term 'Dual Use' in EU Spyware Export Control."

persetujuan dan pengawasan teknologi surveilans, dan memastikan korban pelanggaran memiliki perangkat hukum domestik untuk mendapatkan ganti rugi.³⁵⁵

Selanjutnya Pelapor Khusus menyatakan:³⁵⁶

“Target surveilans mengalami gangguan terhadap hak privasi dan kebebasan berpendapat dan berekspresi mereka, baik upaya surveilans tersebut berhasil atau tidak. Target tidak perlu mengetahui adanya upaya atau keberhasilan intrusi agar gangguan terhadap hak privasi mereka menjadi lengkap.

Gangguan tersebut sebagai bagian dari upaya keseluruhan untuk memberikan konsekuensi kepada target. Jika dilakukan untuk tujuan yang melanggar hukum, upaya surveilans dan operasi yang berhasil dapat digunakan dalam upaya untuk membungkam perbedaan pendapat, memberikan sanksi terhadap kritik.

Dalam atmosfer surveilans ilegal, maka akan membentuk dan membatasi kemampuan mereka untuk menjalankan hak atas kebebasan berekspresi, berasosiasi, berkeyakinan agama, budaya, dan sebagainya.”³⁵⁷

Laporan Kantor Komisioner Tinggi PBB untuk Hak Asasi Manusia untuk hak atas privasi di era digital (*The right to privacy in the digital age*) memperkuat pandangan Pelapor Khusus:³⁵⁸

“Berbagai aktor Negara sering kali tampaknya mengejar tujuan yang tidak sah menurut hukum HAM internasional. Meskipun, dalam keadaan tertentu, tindakan surveilans mungkin diizinkan berdasarkan pasal 17 dan 19 Kovenan Hak-Hak Sipil dan Politik dengan alasan perlindungan keamanan nasional atau ketertiban umum, peretasan tidak pernah dapat dibenarkan untuk alasan politik atau bisnis, yang sering terjadi ketika pembela HAM atau jurnalis menjadi sasaran.

³⁵⁵ David Kaye, *Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, A/HRC/41/35 (Geneva: United Nations, 28 Mei 2019), <https://digitallibrary.un.org/record/3814512>.

³⁵⁶ Kaye, *Surveillance and Human Rights*.

³⁵⁷ Pelapor Khusus merujuk pada Kovenan Hak-Hak Sipil dan Politik dan Deklarasi Universal Hak Asasi Manusia yang melindungi hak setiap orang atas privasi, pendapat, dan ekspresi. Pasal 19 dari kedua instrumen tersebut melindungi hak setiap orang untuk memiliki pendapat tanpa campur tangan dan untuk mencari, menerima, dan menyampaikan informasi dan gagasan dalam segala bentuk, tanpa memandang batas negara dan melalui media apa pun. Pasal 17 (1) Kovenan yang menggemakan pasal 12 Deklarasi, menyatakan bahwa tidak seorang pun boleh dikenai campur tangan sewenang-wenang atau melanggar hukum terhadap privasi, keluarga, rumah, atau korespondensinya. Lihat, Kaye, *Surveillance and Human Rights*.

³⁵⁸ Office of the United Nations High Commissioner for Human Rights (OHCHR), *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights*, A/HRC/51/17 (Geneva: United Nations, 4 Agustus 2022), <https://digitallibrary.un.org/record/3985679>.

Bahkan jika tujuan yang sah sedang dikejar, seperti tujuan keamanan nasional atau perlindungan hak orang lain, penilaian tentang keperluan dan proporsionalitas penggunaan *spyware* sangat membatasi penggunaan *spyware* yang dapat diizinkan. Terdapat argumen kuat piranti seperti Pegasus, yang memungkinkan intrusi tanpa batas ke dalam kehidupan individu dan dapat menjangkau pikiran batin mereka sehingga memengaruhi esensi hak atas privasi dan mengganggu hak absolut atas kebebasan berpikir dan berpendapat.”

Pandangan serupa disampaikan oleh Fionnuala Ní Aoláin, Pelapor Khusus tentang promosi dan perlindungan HAM dan kebebasan mendasar dalam memerangi terorisme (*promotion and protection of human rights and fundamental freedoms while countering terrorism*):³⁵⁹

“Skala pelanggaran HAM yang ditimbulkan oleh proliferasi dan penyalahgunaan teknologi surveilans siber yang canggih dan invasif di seluruh dunia, yang awalnya dibenarkan atau dimaksudkan untuk tujuan kontra-terorisme dan keamanan nasional. Teknologi pengawasan canggih yang dikembangkan untuk tujuan kontra-terorisme dan keamanan nasional semakin menjadi fokus perhatian internasional terkait serangkaian pengungkapan yang menunjukkan piranti tersebut sebenarnya digunakan untuk memata-matai politisi, jurnalis, aktivis HAM, advokat, dan warga negara biasa yang tidak memiliki hubungan dengan terorisme dan tidak menimbulkan ancaman keamanan nasional. Teknologi rahasia yang mengganggu untuk surveilans isi komunikasi digital individu dan informasi lainnya, termasuk metadata (lokasi, durasi, sumber, dan kontak), yang umumnya dikenal sebagai *spyware*, telah berkembang pesat secara internasional di luar kendali dan menimbulkan risiko besar terhadap promosi dan perlindungan HAM.

Dampak surveilans terhadap berbagai HAM sangat besar, maka Pelapor Khusus menekankan bahwa hak atas privasi berfungsi sebagai hak dasar yang melindungi dan memungkinkan banyak hak dan kebebasan lainnya, dan pelindungannya terkait erat dengan keberadaan dan kemajuan masyarakat demokratis. Oleh karena itu, peningkatan penggunaan surveilans rahasia dan pengumpulan informasi konten serta metadata untuk tujuan memerangi terorisme, dikombinasikan dengan perkembangan pesat teknologi baru yang kurang diatur merupakan ancaman signifikan bagi masyarakat demokratis.”

³⁵⁹ Fionnuala Ní Aoláin, *Human Rights Implications of the Development, Use and Transfer of New Technologies in the Context of Counter-Terrorism and Countering and Preventing Violent Extremism: Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, A/HRC/52/39 (Geneva: United Nations, 1 Maret 2023), <https://digitallibrary.un.org/record/4031525>.

Lebih jauh Fionnuala Ní Aoláin mengidentifikasi pelanggaran serius terhadap hukum HAM internasional dalam berbagai akibat penggunaan piranti surveilans, khususnya *spyware*. Pelanggaran tersebut termasuk: (1) pelanggaran hak untuk hidup; (2) paparan kekerasan fisik yang tidak sah, (termasuk kekerasan seksual), penangkapan yang tidak sah, dan/atau pelecehan dari aktor pemerintah atau swasta; (3) campur tangan yang tidak proporsional terhadap hak privasi individu; (4) campur tangan yang tidak proporsional terhadap hak atas kebebasan berekspresi, kebebasan berasosiasi, dan kebebasan beragama; (5) produksi dan penguatan kerugian gender tertentu termasuk kerugian langsung terhadap perempuan dan anak perempuan, serta kelompok minoritas seksual (LGBTQI+); (6) campur tangan terhadap integritas catatan dan bukti dokumenter, yang merusak keadilan prosedural dan supremasi hukum; dan (7) hambatan bagi kemampuan individu untuk memperoleh ganti rugi dan pemulihan yang efektif atas pelanggaran HAM mereka.³⁶⁰

Pandangan senada juga dinyatakan oleh Gina Romero, yang bertindak dalam kapasitas sebagai Pelapor Khusus:³⁶¹

Sistem digital yang invasif, luas, dan berisiko tinggi, yang sering kali secara inheren tidak sesuai dengan kewajiban hak asasi manusia, sering kali dibenarkan secara tidak tepat melalui narasi keamanan dan pencegahan kejahatan. Bahkan sering kali dengan klaim luas yang dikemukakan mengenai keamanan nasional, kedaulatan, terorisme, keselamatan publik, kejahatan transnasional, keamanan siber, kejahatan kebencian, "kejahatan moral", disinformasi, dan sejenisnya. Aktivisme sipil dan politik semakin banyak digunakan sebagai peluang untuk surveilans.

Asosiasi dan perkumpulan sering dilabeli sebagai "ancaman keamanan nasional," "agen asing," "penjahat," atau "teroris." Pihak berwenang menggunakan perpaduan strategi surveilans yang terselubung, tersembunyi, dan online, termasuk pengambilan data, di samping bentuk yang lebih terbuka dan terlihat, seperti drone surveilans. Hal ini menormalisasi pengembangan infrastruktur surveilans yang invasif, termasuk di negara demokrasi

Negara-negara telah mengadopsi langkah-langkah yang terlalu luas yang memperluas surveilans sembari mengabaikan transparansi, pengawasan publik, dan

³⁶⁰ Fionnuala Ní Aoláin, *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach*, position paper (Geneva: Office of the United Nations High Commissioner for Human Rights, April 2023), <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf>

³⁶¹ Gina Romero, *Unmasking the Chilling Effects of the Digital Surveillance Ecosystem: The Erosion of Assembly and Association Rights: Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association*, A/HRC/62/45 (Geneva: United Nations, 21 April 2026), <https://digitallibrary.un.org/record/4113878>.

pelindungan HAM. Pergeseran menuju paradigma preventif ini secara fundamental mengikis asas praduga tak bersalah dan proses hukum yang adil; dengan memaksa individu untuk membuktikan bahwa mereka tidak menimbulkan ancaman. Pada saat bersamaan, Negara secara efektif membalikkan beban pembuktian yang justru memfasilitasi kriminalisasi aktivis secara luas, mengubah lingkungan digital menjadi ruang kecurigaan permanen.”

Pengadilan HAM Eropa (*European Court of Human Rights*) telah menguraikan uji proporsionalitas ini dengan memberikan pelindungan minimum ‘yang harus ditetapkan dalam hukum untuk menghindari penyalahgunaan kekuasaan’ selama operasi surveilans yang ditargetkan. Pada prinsipnya, penggunaan *spyware* untuk tujuan penegakan hukum dan kontra-terorisme dapat mengejar tujuan yang sah, seperti pelindungan keamanan nasional atau ketertiban umum. Dari sudut pandang Pengawas Pelindungan Data Eropa (*European Data Protection Supervisor*), ini hanya akan berlaku untuk situasi ancaman yang sangat serius, seperti serangan teroris yang akan segera terjadi. Lebih jauh, EDPS memperingatkan bahwa kasus-kasus seperti itu bersifat luar biasa dan tidak dapat membenarkan penyebaran teknologi yang sangat invasif secara lebih luas atau sistematis.³⁶²

Oleh karena penggunaan *spyware* berimplikasi pada hak atas hidup, Fionnuala Ní Aoláin merujuk pada Komite Hak Asasi Manusia PBB (*Human Rights Committee*)³⁶³ menyatakan dalam Komentar Umum 36 tentang Hak untuk Hidup (*General Comment 36 on the Right to Life*), 2019 untuk mengartikulasikan tanggung jawab korporasi:³⁶⁴

“Negara harus melakukan uji tuntas untuk melindungi kehidupan individu dari perampasan yang disebabkan oleh individu atau entitas yang perilakunya tidak dapat dikaitkan dengan Negara (*persons or entities whose conduct is not attributable to the State*). Hal ini melibatkan pengambilan langkah-langkah pelindungan khusus terhadap orang-orang dalam situasi rentan yang hidupnya telah ditempatkan pada risiko tertentu karena ancaman khusus atau pola kekerasan yang sudah ada sebelumnya, termasuk pembela HAM, pejabat yang memerangi korupsi dan kejahatan terorganisir, pekerja kemanusiaan, jurnalis, tokoh publik terkemuka, saksi kejahatan dan korban kekerasan dalam rumah tangga dan berbasis gender serta perdagangan manusia.”

³⁶² Riecke, “Unmasking the Term ‘Dual Use’ in EU Spyware Export Control.”

³⁶³ Badan ahli khusus yang bertugas memberikan panduan otoritatif tentang interpretasi standar HAM yang ditetapkan dalam Kovenan Hak-Hak Sipil dan Politik

³⁶⁴ Fionnuala Ní Aoláin dan Adriana Edmeades Jones, “Spyware Out of the Shadows: The Need for a New International Regulatory Approach,” *Just Security*, 16 Mei 2023, <https://www.justsecurity.org/86558/spyware-out-of-the-shadows-the-need-for-a-new-international-regulatory-approach/>.

Kewajiban Negara untuk menghormati dan melindungi kehidupan manusia bahkan lebih jauh lagi, sebagaimana dinyatakan dalam Komentar Umum 36:³⁶⁵

1. Negara-negara pihak harus mengambil langkah-langkah yang tepat untuk melindungi individu dari perampasan nyawa oleh negara lain, organisasi internasional, dan perusahaan asing yang beroperasi di wilayah mereka atau di wilayah lain yang berada di bawah yurisdiksi mereka;
2. Negara juga harus mengambil langkah-langkah legislatif dan langkah-langkah lain yang tepat untuk memastikan bahwa semua kegiatan yang terjadi seluruhnya atau sebagian di wilayah mereka dan di tempat lain yang berada di bawah yurisdiksi mereka, tetapi memiliki dampak langsung dan dapat diperkirakan secara wajar terhadap hak untuk hidup individu di luar wilayah mereka, termasuk kegiatan yang dilakukan oleh badan usaha yang berbasis di wilayah mereka atau yang berada di bawah yurisdiksi mereka, sesuai dengan Pasal 6 Kovenan Hak-Hak Sipil dan Politik dengan mempertimbangkan standar internasional terkait tanggung jawab perusahaan, dan hak korban untuk memperoleh pemulihan yang efektif.

Gina Romero kembali memperkuat tanggung jawab bisnis dalam memperkuat perlindungan HAM yang terdampak penggunaan teknologi surveilans:³⁶⁶

“Di samping kurangnya kemauan politik untuk mengatur teknologi Surveilans berisiko tinggi, yang beberapa di antaranya mungkin secara inheren tidak sesuai dengan kewajiban HAM negara. Hal ini sering kali didorong oleh kolaborasi negara-korporasi yang tidak transparan yang mengabaikan kewajiban HAM, dan tekanan paksa dari negara dan korporasi untuk menghilangkan pengaman yang mencegah penyalahgunaan atau penggunaan yang tidak tepat.”

David Kaye, merekomendasikan moratorium segera terhadap penjualan dan transfer teknologi tersebut sampai peraturan internasional dengan perlindungan HAM diterapkan.³⁶⁷ Rekomendasi ini kemudian dipertegas kembali oleh para ahli HAM PBB³⁶⁸

³⁶⁵ Ní Aoláin dan Edmeades Jones, “Spyware Out of the Shadows.”

³⁶⁶ Romero, *Unmasking the Chilling Effects of the Digital Surveillance Ecosystem*.

³⁶⁷ Kaye, *Surveillance and Human Rights*.

³⁶⁸ Para ahli tersebut Adalah Irene Khan, Pelapor Khusus tentang pemajuan dan perlindungan hak atas kebebasan berekspresi; Mary Lawlor, Pelapor Khusus tentang situasi pembela HAM; Clement Nyaletsossi Voulé, Pelapor Khusus tentang hak atas kebebasan berkumpul secara damai dan berserikat; serta Kelompok Kerja PBB mengenai hak asasi manusia dan perusahaan transnasional serta perusahaan bisnis lainnya (yang dikenal sebagai Kelompok Kerja tentang Bisnis dan Hak Asasi Manusia), yang terdiri dari Surya Deva (Ketua), Elzbieta Karska (Wakil Ketua), Githu Muigai, Dante Pesce, dan Anita Ramasastry. Lihat, Office of the United Nations High Commissioner for Human Rights (OHCHR), “Spyware Scandal: UN Experts Call for Moratorium on Sale of ‘Life Threatening’ Surveillance Tech,” 12 Agustus 2021, <https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening?LangID=E&NewsID=27379>.

yang menyerukan kepada semua Negara untuk memberlakukan moratorium global terhadap penjualan dan transfer teknologi surveilans sampai mereka menerapkan peraturan yang kuat yang menjamin penggunaannya sesuai dengan standar HAM internasional:³⁶⁹

“Sangat berbahaya dan tidak bertanggung jawab untuk membiarkan sektor teknologi dan perdagangan surveilans beroperasi sebagai zona bebas HAM (*human rights-free zone*).

Piranti yang sangat canggih dan mengganggu digunakan untuk memantau, mengintimidasi, dan membungkam para pembela HAM, jurnalis, dan lawan politik. Praktik-praktik tersebut melanggar hak atas kebebasan berekspresi, privasi, dan kebebasan, berpotensi membahayakan nyawa ratusan individu, membahayakan kebebasan media, dan merusak demokrasi, perdamaian, keamanan, dan kerja sama internasional.

Mengingat penghinaan luar biasa terhadap HAM yang ditunjukkan melalui penggunaan surveilans yang luas tersebut, NSO Groups harus mengungkapkan apakah pernah melakukan uji tuntas HAM yang berarti sesuai dengan Prinsip-Prinsip Panduan PBB tentang Bisnis dan Hak Asasi Manusia dan mempublikasikan sepenuhnya temuan dari penyelidikan internal apa pun yang mungkin telah mereka lakukan mengenai masalah ini.

Mendesak Israel, sebagai negara asal NSO Group, untuk mengungkapkan sepenuhnya langkah-langkah apa yang telah mereka ambil untuk meninjau transaksi ekspor NSO mengingat kewajiban HAM yang melekat pada Israel. Hal ini menjadi kewajiban negara untuk memverifikasi bahwa perusahaan seperti Grup NSO tidak menjual atau mentransfer teknologi kepada atau membuat kontrak dengan negara dan entitas yang kemungkinan akan menggunakannya untuk melanggar HAM.”

Amnesty International juga merekomendasikan pentingnya penegakan peraturan terhadap teknologi dwiguna untuk mengatasi proliferasi *spyware* yang sangat invasif dan teknologi surveilans lainnya, yang menimbulkan ancaman serius terhadap HAM. Piranti *spyware* yang sangat invasif tersebut dapat digunakan secara diam-diam untuk melakukan surveilans yang sangat mengganggu terhadap masyarakat sipil, dan menekan kebebasan berekspresi yang dapat menimbulkan efek mengerikan. Tanpa mekanisme penegakan hukum yang efektif, teknologi ini dapat dengan mudah diekspor dan dieksploitasi sehingga menyebabkan pelanggaran dan penyalahgunaan HAM yang mengerikan, termasuk hak atas privasi. Pengembangan teknologi dwiguna bergantung pada komponen dan infrastruktur yang mungkin tidak tunduk pada peraturan

³⁶⁹ OHCHR, “Spyware Scandal: UN Experts Call for Moratorium on Sale of ‘Life Threatening’ Surveillance Tech.”

dwiguna tetapi merupakan bagian integral dari fungsi sistem dengan potensi aplikasi militer.

Selain itu, ketergantungan pada negara-negara yang mengekspor teknologi non-dwiguna yang penting untuk pengoperasian sistem dwiguna semakin menggarisbawahi pentingnya upaya penegakan hukum dalam menegakkan HAM. Dengan memastikan penegakan peraturan yang ketat yang mengatur ekspor dan transfer barang-barang non-dwiguna, pemerintah dapat mencegah proliferasi sistem dwiguna yang mengancam HAM. Upaya kolaboratif antara negara pengekspor dan pengimpor sangat penting untuk membangun kontrol komprehensif yang mencakup seluruh spektrum teknologi yang terlibat dalam sistem dwiguna sehingga mendorong akuntabilitas dan melindungi dari penyalahgunaannya.³⁷⁰

³⁷⁰ Amnesty International, *A Web of Surveillance*.

BAB III

KESIMPULAN DAN REKOMENDASI

Kesimpulan

Perkembangan militerisasi teknologi merupakan proses yang jauh lebih luas daripada sekadar penggunaan teknologi oleh institusi militer. Perkembangan kecerdasan artifisial, drone, teknologi surveilans, *spyware* dan lain sebagainya telah mengubah karakter pertahanan dan keamanan kontemporer. Teknologi yang sebelumnya dikembangkan untuk kepentingan sipil dan komersial dapat dengan cepat diadaptasi untuk fungsi intelijen, pengawasan, identifikasi sasaran, pengambilan keputusan hingga penggunaan kekuatan. Karakter dual-use tersebut membuat pemisahan antara ruang sipil dan militer semakin sulit dipertahankan.

Perubahan tersebut berlangsung bersamaan dengan transformasi kompleks industri-militer (*military-industrial complex*) menjadi ekosistem yang semakin digital. Jika kompleks militer industri klasik menggambarkan hubungan antara pemerintah, institusi militer dan industri persenjataan, perkembangan saat ini memperluas jaringan tersebut dengan masuknya perusahaan teknologi, penyedia cloud, perusahaan AI, produsen chip, perusahaan telekomunikasi, *defence tech start up*, hingga penyedia teknologi pengawasan. Dengan demikian, kapasitas militer di seluruh dunia, saat ini tidak hanya dibangun melalui kepemilikan tank, pesawat tempur atau senjata tetapi melalui penguasaan data, algoritma, sensor, infrastruktur komunikasi dan kemampuan komputasi. Dalam hubungan ini, kebutuhan keamanan menghasilkan anggaran dan pengadaan yang menciptakan pasar bagi industri, sementara kepentingan ekonomi dan kapasitas teknologi industri dapat kembali memengaruhi bagaimana ancaman dan kebutuhan pertahanan didefinisikan.

Dalam konteks Indonesia, gejala tersebut terlihat melalui modernisasi alutsista, peningkatan belanja pertahanan, penguatan industri pertahanan nasional, serta meningkatnya perhatian terhadap AI, sistem nirawak, surveilans dan pertahanan siber. Riset ini menemukan ekosistem militerisasi teknologi terbentuk melalui empat unsur yaitu: (1) teknologi, (2) institusi negara (3), militer, dan (4) industri pertahanan dan swasta/*big tech companies*. Peran militer juga semakin bersinggungan dengan ranah nonmiliter termasuk ruang siber yang tercantum dalam Undang Undang No. 3 Tahun 2025 tentang Perubahan atas Undang Undang No. 34 Tahun 2004 tentang TNI terbaru,

adanya penambahan wewenang dalam Pasal 7 Ayat (2) huruf b angka 15 Operasi Militer Selain Perang (OMSP) tentang Ancaman Pertahanan Siber.

Persoalan HAM ini menjadi semakin penting karena teknologi digital secara fundamental memperbesar kapasitas negara untuk melihat, mengetahui, mengidentifikasi, menghubungkan, mengklasifikasikan, dan mengambil tindakan terhadap individu. Namun, perkembangan kemampuan tersebut belum sepenuhnya diimbangi dengan sistem pengaturan dan pengawasan yang setara. Tantangannya bukan terletak pada seberapa jauh negara mampu mengadopsi teknologi baru, melainkan bagaimana memastikan bahwa peningkatan kapasitas tersebut tidak menghasilkan peningkatan kekuasaan tanpa peningkatan akuntabilitas.

Rekomendasi

Penelitian ini merekomendasikan beberapa hal yang dapat diimplementasikan dalam tatanan nasional. Adapun rekomendasi-rekomendasi tersebut yakni sebagai berikut:

1. Perkuat pengawasan sipil yang substantif terhadap pengadaan dan penggunaan teknologi pertahanan, termasuk melalui Dewan Perwakilan Rakyat (DPR), Komisi Nasional Hak Asasi Manusia (Komnas HAM), dan Ombudsman RI (ORI).
2. Bentuk dasar hukum yang jelas untuk penggunaan teknologi berisiko tinggi seperti *spyware*, *AI surveillance*, biometrik, dan sistem otonom.
3. Mendorong akuntabilitas *Big Technology Companies* dan perusahaan swasta melalui human rights due diligence, audit, serta kejelasan yurisdiksi dan tanggung jawab hukum.
4. Jamin mekanisme pengaduan dan pemulihan yang efektif bagi korban penyalahgunaan teknologi, termasuk *surveillance* ilegal dan pelanggaran berbasis AI.

Daftar Pustaka

- Akbar, Adrial. "Rapat Tertutup di DPR, Menhan-Panglima TNI Usul Tambah Anggaran Rp 184 T." *detikNews*, 9 Juli 2025. <https://news.detik.com/berita/d-8003834/rapat-tertutup-di-dpr-menhan-panglima-tni-usul-tambah-anggaran-rp-184-t>.
- Al Jazeera. "Egypt Blocks Human Rights Watch Website." September 8, 2017. <https://www.aljazeera.com/news/2017/9/8/egypt-blocks-human-rights-watch-website>.
- . "Israel Retrofitting DJI Commercial Drones to Bomb and Surveil Gaza." 8 Mei 2025. <https://www.aljazeera.com/news/2025/5/8/israel-retrofitting-dji-commercial-drones-to-bomb-and-surveil-gaza>.
- Albanese, Francesca. *From Economy of Occupation to Economy of Genocide*. Report of the Special Rapporteur on the Situation of Human Rights in the Palestinian Territories Occupied since 1967. UN Doc. A/HRC/59/23. United Nations, 30 Juni 2025. <https://www.ohchr.org/en/documents/country-reports/ahrc5923-report-special-rapporteur-situation-human-rights-palestinian>.
- . *Report of the Special Rapporteur on the Situation of Human Rights in the Palestinian Territories Occupied since 1967: Gaza Genocide: A Collective Crime*. A/80/492. New York: United Nations, 20 Oktober 2025.
- Amnesty International. *A Web of Surveillance: Unravelling a Murky Network of Spyware Exports to Indonesia*. ASA 21/7974/2024. 1 Mei 2024. <https://www.amnesty.org/en/documents/asa21/7974/2024/en/>.
- . "Indonesia: Military Silences Dissent with Disinformation Campaigns Branding Activists and Journalists 'Foreign Agents'." 19 Mei 2026. <https://www.amnesty.org/en/latest/news/2026/05/indonesia-military-silences-dissent-disinformation-campaigns-branding-activists-journalists-foreign-agents/>.
- . *Membangun Musuh Khayalan: Misinformasi, Disinformasi dan Tuduhan "Antek Asing" di Bawah Presiden Prabowo di Indonesia*. ASA 21/0931/2026. 19 Mei 2026. <https://www.amnesty.org/en/documents/asa21/0931/2026/id/>.
- Amnesty International Indonesia. "'Arus Balik' Hak Asasi Manusia di 100 Hari Pemerintahan Baru." 21 Januari 2025. <https://www.amnesty.id/kabar-terbaru/siaran-pers/arus-balik-hak-asasi-manusia-di-100-hari-pemerintahan-baru/01/2025/>.
- Amnesty International Security Lab dan Citizen Lab. "Devices of Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware." 8 November 2021. <https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/>.

- Angendari, Dewa Ayu Diah. "Militerisme di Media Sosial: Bagaimana UU TNI Mengancam Kebebasan Sipil di Dunia Siber." *The Conversation*. <https://theconversation.com/militerisme-di-media-sosial-bagaimana-uu-tni-mengancam-kebebasan-sipil-di-dunia-siber-254065>.
- Arifianto, Y. *Sistem Pengelolaan Anggaran Belanja Militer di Indonesia: Tinjauan Aspek Pengendalian, Transparansi dan Akuntabilitas Publik*. Tesis magister, Universitas Indonesia, 2005. <https://lib.ui.ac.id/detail?id=83595&lokasi=lokal>.
- ASEAN Parliamentarians for Human Rights (APHR). "Indonesia Must Halt the Import and Use of Highly Invasive Spyware from Israel and Elsewhere, Southeast Asian MPs Say." 6 Mei 2024. <https://aseanmp.org/publications/post/indonesia-must-halt-the-import-and-use-of-highly-invasive-spyware-from-israel-and-elsewhere-southeast-asian-mps-say/>.
- Badan Teknologi Pertahanan Kementerian Pertahanan Republik Indonesia. "Design Requirement Rancang Bangun Weapon Integration System PTTA MALE Konsorsium." 7 Juli 2025. <https://www.kemhan.go.id/batekhan/2025/07/07/design-requirement-rancang-bangun-weapon-integration-system-ptta-male-konsorsium.html>.
- Basu, Arindrajit, dan Gatra Priyandita. "Why Haven't India and Indonesia Signed Up for Anti-Spyware Dialogue?" *Royal United Services Institute*, 10 April 2024. <https://www.rusi.org/explore-our-research/publications/commentary/why-havent-india-and-indonesia-signed-anti-spyware-dialogue>.
- BBC News Indonesia. "Aparat membungkam jurnalis dan aktivis dengan narasi antek asing, sebut laporan." 20 Mei 2026. <https://www.bbc.com/indonesia/articles/cj4pqkw785lo>.
- Bego, Katja. "How a Surge in Defence and Dual-Use Technology Investment Could Reconfigure the Global AI Race." *Chatham House*, 28 April 2026. <https://www.chathamhouse.org/2026/04/how-surge-defence-and-dual-use-technology-investment-could-reconfigure-global-ai-race/02>.
- Breger, Michael. "The Legacies of Militarization: Norman Joshua Writes a Social and Cultural History of Indonesian Authoritarianism." FSI, Stanford University, 17 April 2024. <https://fsi.stanford.edu/news/legacies-militarization-norman-joshua-writes-social-cultural-history-indonesian>.
- Business & Human Rights Resource Centre. "Palantir & Starlink Allegedly Complicit in War Crimes amid Israel's War on Gaza." 6 Juni 2024. <https://www.business-humanrights.org/en/latest-news/palantir-spacex-allegedly-complicit-in-war-crimes-amid-israels-war-in-gaza/>.
- Castells, Manuel. *The Rise of the Network Society*. 2nd ed. Chichester: Wiley-Blackwell, 2010.
- Central Intelligence Agency (CIA). "The Enigma of Alan Turing." 10 April 2015. <https://www.cia.gov/stories/story/the-enigma-of-alan-turing/>.
- Chin Human Rights Organisation (CHRO) dan Myanmar Accountability Project (MAP). "Indonesian Arms Producers Accused of Illegal Sales to Myanmar." 2 Oktober 2023.

<https://progressivevoicemyanmar.org/2023/10/02/press-release-indonesian-arms-producers-accused-of-illegal-sales-to-myanmar>.

CNN Indonesia. "Pemerintah Siapkan Rp329,5 Triliun untuk Pertahanan di RAPBN 2027." 19 Agustus 2026. <https://www.cnnindonesia.com/nasional/20260819113956-20-1393907/pemerintah-siapkan-rp3295-triliun-untuk-pertahanan-di-rapbn-2027>.

Corporate Watch. "What's Driving the Militarisation of Tech—and What We Can Do about It." <https://corporatewatch.org/whats-driving-the-militarisation-of-tech-and-what-we-can-do-about-it/>.

Coveri, Andrea, Claudio Cozza, dan Dario Guarascio. "Big Tech and the US Digital-Military-Industrial Complex." *Intereconomics* 60, no. 2 (2025): 81–87. <https://doi.org/10.2478/ie-2025-0017>.

Cronin-Furman, Kate. *Hypocrisy and Human Rights: Resisting Accountability for Mass Atrocities*. Ithaca, NY: Cornell University Press, 2022.

Damrosch, Lori F. "Gross and Systematic Human Rights Violations." *Max Planck Encyclopedia of Public International Law*. Oxford University Press, 2011. <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1732>.

de Búrca, Gráinne, dan Katharine G. Young. "The (Mis)appropriation of Human Rights by the New Global Right: An Introduction to the Symposium." *International Journal of Constitutional Law* 21, no. 1 (Januari 2023).

Deibert, Ronald J. "Toward a Human-Centric Approach to Cybersecurity." *Ethics & International Affairs* 32, no. 4 (2018): 411–424. <https://doi.org/10.1017/S0892679418000618>.

Deikin, Alexander. *An Alliance of the Monopolies and the Military: On the US Military-Industrial Complex*. Moscow: Novosti Press Agency, 1973.

delle Fave, Danilo. "The Challenges of Dual-Use Space Technologies: The Non-Peaceful Use of Satellites." *Space Generation Advisory Council*, 14 April 2023. <https://spacegeneration.org/the-challenges-of-dual-use-space-technologies-the-non-peaceful-use-of-satellites>.

Defense Advanced Research Projects Agency (DARPA). "AI Next." <https://www.darpa.mil/research/programs/ai-next>.

———. "Breakthrough Technologies for National Security." 2015.

Detik.com. "Rapat Komisi I DPR, Panglima TNI Tertutup Saat Bahas Alutsista." 22 Oktober 2024. <https://news.detik.com/berita/d-5560339/rapat-komisi-i-dpr-panglima-tni-tertutup-saat-bahas-alutsista>.

Deutsche Welle. "Poin-poin Pernyataan Prabowo soal Palestina di KTT PBB." <https://www.dw.com/id/poin-poin-pernyataan-prabowo-soal-palestina-di-ktt-pbb/a-74102466>.

Dragu, Tiberiu, dan Germán Gieczewski. "Strength in Numbers? State Capacity, Military Power and Repression in Authoritarian Regimes." Working paper. New York: Department of Politics, New York University; Princeton: Department of Politics, Princeton University, Maret 2024.

Dwipratama, Gede Priana. "Swarm Drone: Tantangan, Peluang dan Ancaman bagi Indonesia." Direktorat Jenderal Potensi Pertahanan Kementerian Pertahanan Republik Indonesia, 25 April 2024. <https://www.kemhan.go.id/pothan/2024/04/25/swarm-drone-tantangan-peluang-dan-ancaman-bagi-indonesia.html>.

Egliston, Ben, dan Marcus Carter. "The Dangerous Fantasy of Cybernetic Cops." *The MIT Press Reader*, 16 September 2024. <https://thereader.mitpress.mit.edu/the-dangerous-fantasy-of-cybernetic-cops/>.

Eide, Asbjørn. *The Universal Declaration of Human Rights: A Commentary*. Oslo: Scandinavian University Press, 1992.

Elistair. "Intelligence, Surveillance, and Reconnaissance (ISR)." <https://elistair.com/glossary/intelligence-surveillance-reconnaissance/>.

ELSAM. "Peneliti ELSAM Peringatkan Potensi Militerisasi Ruang Digital lewat RUU Keamanan dan Ketahanan Siber (RUU KKS)." 21 Oktober 2025. <https://www.elsam.or.id/teknologi-dan-ham/peneliti-elsam-peringatkan-potensi-militerisasi-ruang-digital-lewat-ruu-keamanan-dan-ketahanan-siber%E2%80%93ruu-kks->.

———. "UU Perlindungan Data Pribadi Mendesak untuk Menjamin Kedaulatan Individu di Ruang Siber." 2025. <https://www.elsam.or.id/siaran-pers/uu-perlindungan-data-pribadi-mendesak-untuk-menjamin-kedaulatan-individu-di-ruang-siber>.

Evron, Yoram, dan Richard A. Bitzinger. *The Fourth Industrial Revolution and Military-Civil Fusion: A New Paradigm for Military Innovation?* Cambridge: Cambridge University Press, 2023.

Faridi, Rushad. "Starlink in Gaza: Humanitarian Lifeline or Military Asset?" *The Daily Star*, 9 September 2025. <https://www.thedailystar.net/slow-reads/focus/news/starlink-gaza-humanitarian-lifeline-or-military-asset-3981756>.

Fatafta, Marwa. "Egypt's New Data Protection Law: Data Protection or Data Control?" *Access Now*, September 24, 2020. <https://www.accessnow.org/egypts-new-data-protection-law-data-protection-or-data-control/>.

Fauzi, Elfian, dan Nabila Alif Radika Shandy. "Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi." *LEX Renaissance* 7, no. 3 (7 Juli 2022): 445–461.

Foreign & Commonwealth Office dan Foreign, Commonwealth & Development Office. "The UK and International Humanitarian Law." GOV.UK. 24 Juli 2018, diperbarui 4 April 2024.

<https://www.gov.uk/government/publications/international-humanitarian-law-and-the-uk-government/uk-and-international-humanitarian-law-2018>.

Freedom House. "Egypt." *Freedom on the Net* 2022. 2022. <https://freedomhouse.org/country/egypt/freedom-net/2022>.

Frenkel, Sheera. "The Militarization of Silicon Valley." *The New York Times*, 4 Agustus 2025. <https://www.nytimes.com/2025/08/04/technology/google-meta-openai-military-war.html>.

Godsin, Manuel. "Rheinmetall Denel Faces Scrutiny over Allegations of Arms Use in Sudan Conflict." *Sunday Independent/The Star*, 8 Juli 2025. <https://thestar.co.za/sundayindependent/news/2025-07-08-rheinmetall-denel-faces-scrutiny-over-allegations-of-arms-use-in-sudan-conflict/>.

González, Roberto J. *How Big Tech and Silicon Valley Are Transforming the Military-Industrial Complex*. Costs of War, Watson Institute for International and Public Affairs, Brown University, 17 April 2024. <https://costsofwar.watson.brown.edu/paper/how-big-tech-and-silicon-valley-are-transforming-military-industrial-complex>.

Goodman, Matthew P., Matthew Reynolds, dan Julianne Fittipaldi. *Economic Security in Emerging Markets: A Look at India, Vietnam, and Indonesia*. CSIS Brief. Washington, DC: Center for Strategic and International Studies (CSIS), 17 Mei 2022. <https://www.csis.org/analysis/economic-security-emerging-markets-look-india-vietnam-and-indonesia>.

Gorbanova, Mariya, dan Leah Wawro. *The Transparency of National Defence Budgets: An Initial Review*. London: Transparency International UK, 2011.

Hafiez, Fachri Audhia. "Rapat Bahas Anggaran Alutsista Menhan dengan Komisi I DPR Digelar Tertutup." *MetroTVNews.com*, 12 Juni 2024. <https://www.metrotvnews.com/read/bD2C1Qj6-rapat-bahas-anggaran-alutsista-menhan-dengan-komisi-i-dpr-digelar-tertutup>.

Haripin, Muhamad. *Civil-Military Relations in Indonesia: The Politics of Military Operations Other Than War*. Abingdon: Routledge, 2020.

———. "Indonesian Parliament Passes Law Expanding Military's Role in Government." *ADRN Issue Briefing*, 17 April 2025. <http://adrnresearch.org/publications/list.php?cid=2&idx=407&ckattempt=3>.

Haripin, Muhamad, Adhi Priamarizki, dan Leonard C. Sebastian. "Introduction: Reform Setbacks and Selective Emulation—The Path to Military Modernisation in Indonesia." Dalam *Military Modernisation and Civil-Military Relations in Indonesia*, disunting oleh Muhamad Haripin, Adhi Priamarizki, dan Leonard C. Sebastian, 1–14. Singapore: Palgrave Macmillan, 2025.

Haripin, Muhamad, dan Adhi Priamarizki. "Jokowi Consolidates Influence over TNI as Elections Loom." *New Mandala*. <https://www.newmandala.org/jokowi-consolidates-influence-over-tni-as-elections-loom/>.

- Harsono, Hugh. "Indonesia's Haphazard Military Acquisitions Risks Its Global Ambitions." *Small Wars Journal*, 29 September 2025. <https://smallwarsjournal.com/2025/09/29/indonesia-military-acquisitions-global-ambitions/>.
- Harun, Umar. *Perkembangan Politik Internasional Era Perang Dingin dan Globalisasi*. Jakarta: Lembaga Penerbitan Universitas Nasional, 2022.
- Hasiana, Dovana. "Anggaran Pertahanan 2025 Dipatok Naik 47% Jadi Rp245 Triliun." *Bloomberg Technoz*, 6 Juli 2025. <https://www.bloombergtechnoz.com/detail-news/76302/anggaran-pertahanan-2025-dipatok-naik-47-jadi-rp245-triliun>.
- Henschke, Adam. *Ethics in an Age of Surveillance: Personal Information and Virtual Identities*. Cambridge: Cambridge University Press, 2017.
- Hinton, James W. *Dual-Use Technologies in the Age of Intangibles*. Policy Brief No. 215. Waterloo, ON: Centre for International Governance Innovation (CIGI), 3 November 2025. <https://www.cigionline.org/publications/dual-use-technologies-in-the-age-of-intangibles/>.
- Human Rights Watch. *Looking the Other Way: EU Failure to Prevent Surveillance Exports to Rights Violators*. 12 Mei 2026. <https://www.hrw.org/report/2026/05/12/looking-the-other-way/eu-failure-to-prevent-surveillance-exports-to-rights>.
- . "Myanmar: Facial Recognition System Threatens Rights: Camera Surveillance, Mass Data Collection Bolsters Abusive Junta." 12 Maret 2021. <https://www.hrw.org/news/2021/03/12/myanmar-facial-recognition-system-threatens-rights>.
- Ikrom, Moh Bagus Fadhli Dzil, dan Badrut Tamam. "Perlindungan Hukum Hak Privasi Warga Negara terhadap Kebocoran Data Pribadi di Indonesia." *Constitution Journal* 3, no. 2 (Desember 2024).
- Indonesia Defense. "Spesifikasi Drone Baru untuk Tugas Operasi Prajurit Marinir di Perbatasan." 17 April 2024. <https://indonesiadefense.com/spesifikasi-drone-baru-untuk-tugas-operasi-prajurit-marinir-di-perbatasan/>.
- International Committee of the Red Cross. "Methods and Means of Warfare."
- . *Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach*. June 2019.
- Jili, B. "The Rise of Chinese Surveillance Technology in Africa." Electronic Privacy Information Center (EPIC), May 31, 2022. <https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa/>.
- Kementerian Luar Negeri Republik Indonesia. "Indonesia dan Negara-Negara Afrika Tandatangani MoU Industri Strategis di IAF 2024." 3 September 2024. <https://kemlu.go.id/berita/indonesia-dan-negara-negara-afrika-tandatangani-mou-industri-strategis-di-iaf-2024>.

Kementerian Pertahanan Republik Indonesia. "Unhan RI Sukses Luncurkan Satelit Nano Indonesia, RIDU-Sat 1." 25 Juni 2025. <https://www.kemhan.go.id/2025/06/25/unhan-ri-sukses-luncurkan-satelit-nano-indonesia-ridu-sat-1.html>.

Keselman, Gene, dan Fiona Murray. "Dual-Use Is a Strategy, Not a Category (Nor a Trap)." *War on the Rocks*, 2 Januari 2025. <https://warontherocks.com/dual-use-is-a-strategy-not-a-category-nor-a-trap/>.

Komite Kebijakan Industri Pertahanan (KKIP). "Rencana Aksi Industri Pertahanan: Penguasaan Sepuluh Teknologi Prioritas." 20 Februari 2023. <https://www.kkip.go.id/2023/02/20/rencana-aksi-industri-pertahanan-penguasaan-sepuluh-teknologi-prioritas/>.

———. "Sejarah Industri Pertahanan Nasional." <https://www.kkip.go.id/sejarah>.

Kompas.com. "Kemenhan Bentuk Badan Baru, Diminta Pastikan Tidak Ada Tumpang Tindih." 8 Agustus 2025. <https://nasional.kompas.com/read/2025/08/08/20124741/kemenhan-bentuk-badan-baru-diminta-pastikan-tidak-ada-tumpang-tindih>.

Kompas.id. "Kadispenad: Kontrak Monitoring Medsos Rp 49,2 Miliar Tidak Pernah Dilaksanakan." 30 April 2026. <https://www.kompas.id/artikel/kadispenad-kontrak-monitoring-medsos-rp-492-miliar-tidak-pernah-dilaksanakan>.

———. "Publik Pertanyakan Anggaran Rp 49,2 Miliar untuk Monitoring Medsos TNI AD." 29 April 2026. <https://www.kompas.id/artikel/anggaran-rp-492-miliar-untuk-monitoring-medsos-tni-ad-dipertanyakan-publik>.

Kuntsman, Adi, dan Rebecca L. Stein. *Digital Militarism: Israel's Occupation in the Social Media Age*. Redwood City: Stanford University Press, 2015.

Lamensch, Marie. "Authoritarianism Has Been Reinvented for the Digital Age." *Centre for International Governance Innovation*, 9 Juli 2021. <https://www.cigionline.org/articles/authoritarianism-has-been-reinvented-for-the-digital-age/>.

Lassman, Thomas C. "Putting the Military Back into the History of the Military-Industrial Complex: The Management of Technological Innovation in the U.S. Army, 1945–1960." *Isis* 106, no. 1 (2015): 94–120. <https://doi.org/10.1086/681038>.

Ledbetter, James. *Unwarranted Influence: Dwight D. Eisenhower and the Military-Industrial Complex*. New Haven, CT: Yale University Press, 2011.

Liang, Xiao, Nan Tian, Diego Lopes da Silva, Lorenzo Scarazzato, Zubaida Karim, dan Jade Guiberteau Ricard. "Trends in World Military Expenditure, 2025." *SIPRI Fact Sheet*. Stockholm International Peace Research Institute (SIPRI), April 2026.

Lindsey, Tim. "Indonesia's New President, Prabowo Subianto, Finds Democracy 'Very Tiring'. Are Darker Days Ahead for the Country?" *The Conversation*, 18 Oktober 2024. <https://theconversation.com/indonesias-new-president-prabowo-subianto-finds-democracy-very-tiring-are-darker-days-ahead-for-the-country-241256>.

- Loewenstein, Antony. *The Palestine Laboratory: How Israel Exports the Technology of Occupation Around the World*. London: Verso, 2023.
- Lopes, Gonçalo. "From Orbit to Cyber Wars: The New Era of Civil-Military Synergy." *VisionSpace*, 25 Maret 2025. <https://visionspace.com/from-orbit-to-cyber-wars-the-new-era-of-civil-military-synergy/>.
- LP3ES. "Membangun Resiliensi Masyarakat Sipil Setelah 27 Tahun Reformasi." May 22, 2025. <https://www.lp3es.or.id/2025/05/22/membangun-resiliensi-masyarakat-sipil-setelah-27-tahun-reformasi/>.
- Luckey, David, et al. *Measuring Intelligence, Surveillance, and Reconnaissance Effectiveness at the United States Central Command*. Santa Monica, CA: RAND Corporation, 2021.
- Lyon, David. *The Culture of Surveillance: Watching as a Way of Life*. Cambridge: Polity Press, 2018. <https://www.perlego.com/book/1536337/the-culture-of-surveillance-watching-as-a-way-of-life-pdf>.
- Macaluso, Alyssa. "Space Is Not a Human Rights Vacuum." *Science & Politics*, 25 Februari 2026. <https://sciencepolitics.org/2026/02/25/space-is-not-a-human-rights-vacuum/>.
- Mambrini, Tommaso. "Dual-Use Technologies in the Rise of the Space Economy." *Berkeley Technology Law Journal*, 28 April 2026. <https://btlj.org/2026/04/dual-use-technologies-in-the-rise-of-the-space-economy/>.
- Mann, Tim. "Activists on Trial: The Weaponisation of Online Defamation Provisions in Indonesia." *Australian Journal of Asian Law* 25, no. 2 (2025): 1–16.
- Mantalean, Vitorio, dan Ardito Ramadhan. "Imparsial: Pengadaan Alutsista Rawan Korupsi dengan Dalih Rahasia Pertahanan." *Kompas.com*, 10 Desember 2024.
- Mathe, Zen, dan Caryn Dolley. "Unaccountable 0004: Rheinmetall Denel Munition: Murder and Mayhem in Yemen." *Open Secrets*, 22 Januari 2020. <https://www.opensecrets.org.za/rheinmetall-denel-munition-murder-and-mayhem-in-yemen/>.
- McConnell, B. "How Cyberspace Is at the Leading Edge of Global Change." *The Diplomat*, February 25, 2016. <https://thediplomat.com/2016/02/how-cyberspace-is-at-the-leading-edge-of-global-change>.
- Mengko, Diandra Megaputri, dan Aulia Fitri Rosadi. "Non-Institutionalised Civilian Control and Military Operations Other than War in Indonesia." Dalam *Military Modernisation and Civil-Military Relations in Indonesia*, disunting oleh Muhamad Haripin, Adhi Priamarizki, dan Leonard C. Sebastian. Singapore: Palgrave Macmillan, 2025.
- Michaelsen, Marcus. *The Digital Transnational Repression Toolkit, and Its Silencing Effects*. Freedom House, 2020. <https://freedomhouse.org/report/special-report/2020/digital-transnational-repression-toolkit-and-its-silencing-effects>.

- Mietzner, Marcus. "The Military's Transformation from Praetorian Ruler to Presidential Coalition Partner." Dalam *Oxford Research Encyclopedia of Politics*, disunting oleh Erin Hannah. New York: Oxford University Press, 2020.
- Miller, Seumas. *Dual Use Science and Technology, Ethics and Weapons of Mass Destruction*. Cham: Springer, 2018.
- Ministry of Foreign Affairs of Pakistan. "Joint Statement by the Foreign Ministers of Jordan, United Arab Emirates, Indonesia, Pakistan, Türkiye, Saudi Arabia, Qatar and Egypt." <https://mofa.gov.pk/press-releases/joint-statement-by-the-foreign-ministers-of-jordan-united-arab-emirates-indonesia-pakistan-turkiye-saudi-arabia-qatar-and-egypt>.
- Mills, C. Wright. *The Power Elite*. New York: Oxford University Press, 1956.
- MIT Mission Innovation X (MIx). "Defining 'Dual-Use.'" *Dual-Use Readiness Model*. <https://dualuse.mit.edu/defining-dual-use/>.
- Muir, Laura. "Control Space?: Cinematic Representations of Surveillance Space between Discipline and Control." *Urban Surveillance* 9, no. 3 (2012): 263–279.
- Munthaha, Dwi. "Militer Era Prabowo: Pretorianisme Baru?" *Kompas.id*, 20 Agustus 2025. <https://www.kompas.id/artikel/militer-era-prabowo-pretorianisme-baru>.
- NATO. *Summary of NATO's Revised Artificial Intelligence (AI) Strategy*. 10 Juli 2024. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy>.
- Neumann, Isabella. "It Is Complicated: Cyber into the Civil–Military Relationship." *Journal of Cybersecurity* 12, no. 1 (2026): 1–12. <https://doi.org/10.1093/cybsec/tyag012>.
- New Internationalist. "How Palestine Became Israel's Spyware Test-Bed." <https://newint.org/features/2023/10/02/spy-games>.
- Ní Aoláin, Fionnuala, dan Adriana Edmeades Jones. "Spyware Out of the Shadows: The Need for a New International Regulatory Approach." *Just Security*, 16 Mei 2023. <https://www.justsecurity.org/86558/spyware-out-of-the-shadows-the-need-for-a-new-international-regulatory-approach/>.
- Ní Aoláin, Fionnuala. *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach*. Position paper. Geneva: Office of the United Nations High Commissioner for Human Rights, April 2023. <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf>.
- Niiles, Sofia. "Dual-Use Satellites and the Law of Armed Conflict: The Tension Between Targeting Rules and State Responsibility in Outer Space." *Amsterdam Law Forum*, 10 Juni 2026. <https://vu.nl/en/news/2026/dual-use-satellites-and-the-law-of-armed-conflict>.

- Nugraha, Taufik Rachmat, dan Bich Tran. *Bridging the Legal and Strategic Mismatch in the Indonesian Air Force's Space Unit*. IDSS Paper IP26100. Singapore: S. Rajaratnam School of International Studies, Nanyang Technological University, 27 Agustus 2026. <https://rsis.edu.sg/rsis-publication/idss/ip26100-bridging-the-legal-and-strategic-mismatch-in-the-indonesian-air-forces-space-unit/>.
- Office of the United Nations High Commissioner for Human Rights (OHCHR). "UN Experts Condemn 'Board of Peace,' Call for a Reparative, Rights-Based Approach to Reconstruction in Gaza." <https://www.ohchr.org/en/special-procedures/sr-housing/mr-balakrishnan-rajagopal>.
- . Special Procedures. "Communication to Rheinmetall AG." Ref. AL OTH 81/2024. 17 May 2024. <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=29082>.
- Peron, A. E. dos R., D. Almstadter Mattar de Magalhães, and G. F. Caetano. "Beyond Digital Repression: Techno-Authoritarianism in Radical Right Governments." *Cogent Social Sciences* 11, no. 1 (2025). <https://doi.org/10.1080/23311886.2025.2528457>.
- Piovesan, Giorgia. "Digital Authoritarianism in the Middle East." *The Security Distillery*, April 19, 2023. <https://thesecuritydistillery.org/all-articles/digital-authoritarianism-in-the-middle-east>.
- Poetranto, Irene. "Techno-Legal Internet Controls in Indonesia and Their Impact on Free Expression." Dalam *Digital Democracy in a Divided Global Landscape*, 35–38. Washington, DC: Carnegie Endowment for International Peace, 2025.
- . "The Architecture of Digital Repression: Internet Service Providers Can Facilitate Internet Access but Also Draconian Control." *Carnegie Endowment for International Peace*, 10 Maret 2026. <https://carnegieendowment.org/research/2026/03/the-architecture-of-digital-repression>.
- Polyakova, Alina, dan Chris Meserole. *Exporting Digital Authoritarianism: The Russian and Chinese Models*. Washington, DC: Brookings Institution, 2019.
- Priamarizki, Adhi, dan Edna Caroline. *Prabowo's Defence Challenge: Making "Triple Helix" Work*. IDSS Paper IP26067. Singapore: S. Rajaratnam School of International Studies, Nanyang Technological University, 21 Mei 2026. <https://rsis.edu.sg/rsis-publication/idss/ip26067-prabowos-defence-challenge-making-triple-helix-work/>.
- Privacy International. "Challenging the Militarisation of Tech." <https://privacyinternational.org/campaigns/militarisation-of-tech>.
- . "State of Privacy: Egypt." January 26, 2019. <https://www.privacyinternational.org/state-privacy/1001/state-privacy-egypt>.
- . "What Is Militarisation of Tech?" 12 September 2025. <https://privacyinternational.org/long-read/5668/what-militarisation-tech>.

- Privacy International dan ELSAM. *Privasi 101: Panduan Memahami Privasi, Perlindungan Data, dan Surveilans Komunikasi*. Jakarta: ELSAM dan Privacy International, 2015.
- Privacy International dan PAX. *Tech Giants, the Arms Industry and the Weaponisation of AI: When Algorithms Go to War*. June 2026.
- Priyandita, Gatra, dan Christian Guntur Lebang. "Indonesia's Cyber Soldiers: Armed without a Compass." *The Strategist*, 11 April 2025. <https://www.aspistrategist.org.au/indonesias-cyber-soldiers-armed-without-a-compass/>.
- Probasco, Emelia, Helen Toner, Matthew Burtell, dan Tim G. J. Rudner. "AI for Military Decision-Making: Harnessing the Advantages and Avoiding the Risks." Center for Security and Emerging Technology, April 2025. <https://doi.org/10.51593/20240028>.
- PT Dahana. "Dahana–RDM Sepakati Pembangunan Fasilitas *Energetic Material* di Indonesia." 25 November 2025. <https://dahana.id/id/dahana-rdm-sepakati-pembangunan-fasilitas-energetic-material-di-indonesia/>.
- PT Pindad (Persero). "Pindad Bersiap Menjadi Produsen Munisi Global." 8 Agustus 2014. <https://pindad.com/pindad-bersiap-menjadi-produsen-munisi-global>.
- . "Kendarai Ranops Maung, Presiden Tinjau Divisi Munisi dan Apresiasi Kemampuan Lini Produksi PT Pindad." 27 Juli 2023. <https://pindad.com/kendarai-ranops-maung-presiden-tinjau-divisi-munisi-dan-apresiasi-kemampuan-lini-produksi-pt-pindad>.
- Rafiq, Aamna. "Militarisation of Artificial Intelligence and Future of Arms Control in South Asia." *Strategic Studies* 41, no. 2 (2021): 49–63.
- Rahmawati, Dwi. "Bahas Anggaran Kemhan 2025, Rapat Komisi I DPR Digelar Tertutup." *detikNews*, 12 Juni 2024. <https://news.detik.com/berita/d-7386957/bahas-anggaran-kemhan-2025-rapat-komisi-i-dpr-digelar-tertutup>.
- Rakhmat, Muhammad Zulfikar. "Indonesia Cannot Condemn Gaza Genocide While Still Silent on Its Use of Israeli Spyware." *Middle East Monitor*, 30 September 2025. <https://www.middleeastmonitor.com/20250930-indonesia-cannot-condemn-gaza-genocide-while-still-silent-on-its-use-of-israeli-spyware/>.
- Remanu, Alifah Jasmine Kallista, Calista Sahlah Purwanto, Nadhira Nurul Fajri, dan Firman. "Analisis Implikasi UU ITE terhadap Kebebasan Berekspresi di Ruang Digital: Studi Kasus Greenpeace Indonesia." *Jurnal ISO: Jurnal Ilmu Sosial, Politik dan Humaniora* 4, no. 2 (2024).
- Reporters Without Borders (RSF). "Egypt's New Cybercrime Law Legalizes Internet Censorship." August 21, 2018. <https://rsf.org/en/egypt-s-new-cybercrime-law-legalizes-internet-censorship>.
- Reuters. "Indonesian Officials Targeted by Spyware: Sources." *Al Jazeera*, 30 September 2022. <https://www.aljazeera.com/economy/2022/9/30/indonesian-officials-targeted-by-spyware-sources>.

- Riecke, Lena. "Unmasking the Term 'Dual Use' in EU Spyware Export Control." *European Journal of International Law* 34, no. 3 (2023): 697–720. <https://doi.org/10.1093/ejil/chad039>.
- Rheinmetall. "Rheinmetall Denel Munition (Pty) Ltd." <https://www.rheinmetall.com/en/company/subsidiaries/rheinmetall-denel-munition>.
- Ritonga, Machradin Wahyudi. "Dinilai Cederai Demokrasi, Wewenang TNI dalam RUU Keamanan dan Ketahanan Siber Jadi Sorotan." *Kompas.id*, 4 Oktober 2025. <https://www.kompas.id/artikel/dinilai-cederai-demokrasi-wewenang-tni-dalam-ruu-keamanan-dan-ketahanan-siber-jadi-sorotan>.
- Rogers, James Patton. "Introduction: Why Study Drones?" Dalam *De Gruyter Handbook of Drone Warfare*, diedit oleh James Patton Rogers, 1–?. Berlin/Boston: De Gruyter, 2024.
- Romero, Gina. *Protecting the Rights to Freedom of Peaceful Assembly and of Association from Stigmatization*. Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association. UN Doc. A/79/263. United Nations, 31 Juli 2024. https://digitallibrary.un.org/record/4059940/files/A_79_263-EN.pdf.
- . *Unmasking the Chilling Effects of the Digital Surveillance Ecosystem: The Erosion of Assembly and Association Rights: Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association*. A/HRC/62/45. Geneva: United Nations, 21 April 2026. <https://digitallibrary.un.org/record/4113878>.
- Rosner, Robert. "Preface." Dalam *Governance of Dual-Use Technologies: Theory and Practice*, disunting oleh Elisa D. Harris. Cambridge, MA: American Academy of Arts and Sciences, 2016.
- Saraçoğlu, Diyar. "From Productive Force to Destructive Force: Digital Colonialism in Palestine." *bianet*, 7 Oktober 2025. <https://bianet.org/yazi/from-productive-force-to-destructive-force-digital-colonialism-in-palestine-312332>.
- Schäfer, Saskia, dan Daniel Peterson. "Appropriations of Human Rights Discourses: Evidence from Indonesia and Malaysia." *International Journal of Constitutional Law* 24, no. 1 (Januari 2026).
- Setiawan, Ken M. P. "A State of Surveillance? Freedom of Expression under the Jokowi Presidency." Dalam *Democracy in Indonesia: From Stagnation to Regression?*, disunting oleh Thomas Power dan Eve Warburton. Singapore: ISEAS–Yusof Ishak Institute, 2020.
- Shaheen, Rubina. "Gender and Surveillance: The Implications of Biometric Technologies for Privacy and Equity." *Journal of Gender, Power, and Social Transformation* 1, no. 3 (2024).
- Shin, Beomchul. *The Republic of Korea's Perspective on Defense Transparency*. Policy Brief No. 2011-1. Northeast Asia Defense Transparency Project, University of California Institute on Global Conflict and Cooperation, Oktober 2011.

- Shpak, Valerij. "Indirect Praetorianism: The Case of Turkey's Military." *Scientific Journal of the Military University of Land Forces* 54, no. 4(206) (2022): 624–638. <https://doi.org/10.5604/01.3001.0016.0757>.
- Sinha, Bappa. "Big Tech's Deep Links with Genocide in Gaza." *NewsClick*, 6 Oktober 2025. <https://www.newsclick.in/big-techs-deep-links-genocide-gaza>.
- South China Morning Post. "Facial Recognition Is Used in China for Everything from Refuse Collection to Toilet Paper Dispensers and Its Citizens Are Growing Increasingly Alarmed, Survey Shows." 2021. <https://www.scmp.com/tech/innovation/article/3119281/facial-recognition-used-china-everything-refuse-collection-toilet>.
- Southeast Asia Freedom of Expression Network (SAFEnet). *Laporan Situasi Hak-hak Digital Indonesia 2020: Represi Digital di Tengah Pandemi*. Denpasar: Southeast Asia Freedom of Expression Network (SAFEnet), 2021.
- . "Pernyataan Sikap SAFEnet: Tolak RUU TNI, Tolak Militerisasi Ruang Siber." 17 Maret 2025. <https://safenet.or.id/id/2025/03/tolak-ruu-tni-tolak-militerisasi-ruang-siber/>.
- Stellpflug, Timo. "The Resurgence of European and UK Defence Tech: Markets, Technology, and Investment." *Taylor Wessing*, July 31, 2025. <https://www.taylorwessing.com/en/interface/2025/defence-tech/the-resurgence-of-european-and-uk-defence-tech>.
- Stockholm International Peace Research Institute (SIPRI). "Unprecedented Rise in Global Military Expenditure as European and Middle East Spending Surges." *Press Release*, 28 April 2025. <https://www.sipri.org/media/press-release/2025/unprecedented-rise-global-military-expenditure-european-and-middle-east-spending-surges>.
- Tangredi, Sam J., dan George Galdorisi, eds. *AI at War: How Big Data, Artificial Intelligence, and Machine Learning Are Changing Naval Warfare*. Annapolis, MD: Naval Institute Press, 2021.
- Tempo. "Cerita Kepala Desa soal Peran Tentara di Kopdes Merah Putih." 16 Februari 2026. <https://www.tempo.co/politik/cerita-kepala-desa-soal-peran-tentara-di-kopdes-merah-putih-2115459>.
- . "Demokrasi Santun Prabowo Subianto." 23 Oktober 2024. <https://www.tempo.co/kolom/demokrasi-santun-prabowo-subianto-1096274>.
- . "Jokowi Pamer Pegang Data Intelijen Arah Parpol, Begini Bunyi Pasal 1 dan 2 UU Nomor 17 Tahun 2011 tentang Intelijen Negara." 20 September 2023. <https://www.tempo.co/politik/jokowi-pamer-pegang-data-intelijen-arrah-parpol-begini-bunyi-pasal-1-dan-2-uu-nomor-17-tahun-2011-tentang-intelijen-negara-141871>.
- . "Koperasi Desa Merah Putih." *Tempo.co*. <https://www.tempo.co/tag/koperasi-desa-merah-putih>.

———. “Menhan: Kebutuhan Anggaran Pertahanan Tahun 2027 Rp 667 Triliun.” <https://www.tempo.co/politik/menhan-kebutuhan-anggaran-pertahanan-tahun-2027-rp-667-triliun-2266159>.

Tempo Editorial. “The Dark Threat of Surveillance Equipment.” *Tempo.co*, 9 Mei 2024. <https://en.tempo.co/read/1865183/the-dark-threat-of-surveillance-equipment>.

Tian, Nan, dan Xiao Liang. *Rebalancing Military Spending Towards Achieving Sustainable Development*. SIPRI Research Policy Paper. Stockholm: Stockholm International Peace Research Institute (SIPRI), November 2025. <https://doi.org/10.55163/ZCIE5196>.

U.S. Central Command. “About Us.” <https://www.centcom.mil/ABOUT-US/>.

U.S. Department of Defense. “Project Maven Industry Day Pursues Artificial Intelligence for DoD Challenges.” 3 November 2017.

———. “Project Maven to Deploy Computer Algorithms to War Zone by Year’s End.” 21 Juli 2017.

Ufen, Andreas. “The Rise of Digital Repression in Indonesia under Joko Widodo.” *GIGA Focus Asia*, no. 1 (Januari 2024). <https://doi.org/10.57671/gfas-24012>.

UN B-Tech Project, Heartland Initiative, Business & Human Rights Resource Centre, dan Open MIC. “Key Takeaways: Dual-Use Dominance When Every Innovation Has a Defense Application.” 26 Juli 2025. <https://www.ohchr.org/sites/default/files/documents/form/defense-application-key-takeaways-25-internet-governance-forum-side-event-dual-use-dominance-innovation-1-en.pdf>.

United Nations. Secretary-General. *The Security We Need: Rebalancing Military Spending for a Sustainable and Peaceful Future: Report of the Secretary-General on the Impact of the Global Increase in Military Expenditure on the Achievement of the Sustainable Development Goals as Requested by Action 13(c) of the Pact for the Future*. 2025. https://digitallibrary.un.org/record/4088022/files/SG_Report_TheSecurityWeNeed.pdf.

University World News. “Indonesia Ramps Up Space R&D to Reduce Foreign Reliance.” 25 November 2025. <https://www.universityworldnews.com/post.php?story=20251125121827251>.

Vaseashta, Ashok, dan Alvaro Rocha, eds. *Spectrum of Dual-Use Technologies: Unforeseen Risks Versus Returns*. Cham: Springer Nature Switzerland, 2026. <https://doi.org/10.1007/978-3-032-00202-0>.

VOA Indonesia. “Perketat Pengawasan, Junta Myanmar Pasang CCTV Canggih China di Lebih Banyak Kota.” 7 Juli 2022. <https://www.voaindonesia.com/a/perketat-pengawasan-junta-myanmar-pasang-cctv-canggih-china-di-lebih-banyak-kota-/6653414.html>.

War on Want. “Israeli Spyware Is Threatening Our Rights and Freedoms.” <https://waronwant.org/resources/israeli-spyware-threatening-our-rights-and-freedoms>.

- Waters, Nick. "First ISIS, then Iraq, now Israel: IDF Use of Commercial Drones." *Bellingcat*, 18 Juni 2018. <https://www.bellingcat.com/news/middle-east/2018/06/18/first-isis-iraq-now-israel-idf-use-commercial-drones/>.
- Widyatama, Elvan. "Gila-Gilaan! AS Habiskan Rp6.000 T Buat Teknologi Perang Masa Depan." *CNBC Indonesia*, November 13, 2025. <https://www.cnbcindonesia.com/research/20251112105824-128-684492/gila-gilaan-as-habiskan-rp6000-t-buat-teknologi-perang-masa-depan>.
- Wijayanto. "Masyarakat Sipil dan Represi Digital." *Kompas*, 10 Juni 2025. <https://www.kompas.id/artikel/melindungi-masyarakat-sipil-dari-represi-digital-2>.
- Willoughby, Angus. "Biometric Surveillance and the Right to Privacy." 5 Oktober 2017. <https://technologyandsociety.org/biometric-surveillance-and-the-right-to-privacy/>.
- Wingender, Asger Mose, dan Søren Bang. "Modern Arms Technologies Help Autocratic Rulers Stay in Power." *University of Copenhagen*, 25 Januari 2023. https://news.ku.dk/all_news/2023/01/modern-arms-technologies-help-autocratic-rulers-stay-in-power.
- Withrington, Claire. "The Internet of Military Things." August 24, 2023. <https://cove.army.gov.au/article/internet-military-things>.
- Yilmaz, Ihsan, Ali Mamouri, Shahram Akbarzadeh, dan Muhammad Omer. *Authoritarian Diffusion in the Cyberspace: How Egypt Learns, Emulates, and Cooperates in Digital Authoritarianism*. Brussels: European Center for Populism Studies, 2025. <https://doi.org/10.55271/rp0097>.
- Yousef, Mohammad. "Why the Recent UNSC Resolution 2803 'Board of Peace' Violates the UN Charter." *Middle East Monitor*, 21 November 2025. <https://www.middleeastmonitor.com/20251121-why-the-recent-unsc-resolution-2803-board-of-peace-violates-the-un-charter/>.



Sejak berdiri pada 14 Agustus 1993, Lembaga Studi dan Advokasi Masyarakat (ELSAM) telah mengembangkan strategi untuk menggabungkan metode kerja organisasi think tank dan gerakan hak asasi manusia (HAM), dalam operasionalnya. Karakter inilah yang membuat ELSAM unik, sebagai think tank berbasis gerakan, dengan dua fokus utama: studi menggunakan pendekatan berbasis hak, dan melakukan advokasi kebijakan. ELSAM berupaya untuk terus mendorong hadirnya kebijakan berbasis bukti untuk memperkuat penghormatan, pemenuhan, dan perlindungan HAM.

Pembentukan ELSAM dimaksudkan untuk mencapai tujuan mewujudkan tatanan masyarakat yang berpegang pada nilai-nilai hak asasi manusia, keadilan dan demokrasi. Dalam mencapai tujuan tersebut, ELSAM mengembangkan setidaknya empat kegiatan utama: (1) studi dan produksi pengetahuan HAM untuk mendukung advokasi kebijakan; (2) pengarusutamaan HAM dalam pembentukan kebijakan; (3) advokasi hukum untuk mendorong perubahan kebijakan, termasuk melalui sarana litigasi strategis; dan (4) penyelenggaraan berbagai pendidikan HAM, dengan variasi topik dan target audiensi yang beragam.

Berbagai kegiatan utama di atas terutama diaplikasikan dalam sejumlah area topik strategis ELSAM, yang memfokuskan diri pada isu: (1) HAM dan Teknologi, terutama merespons kecepatan inovasi teknologi digital yang berdampak luas bagi HAM; (2) HAM dan Bisnis, mengingat semakin besarnya peran korporasi dalam mempengaruhi relasi antara pemegang hak dan pemangku kewajiban; (3) HAM dan Lingkungan, penting menekankan keberlanjutan lingkungan sebagai bagian dari HAM; (4) Kebebasan Dasar, terutama kebebasan berekspresi, kebebasan beragama/berkeyakinan, dan kebebasan berkumpul/berserikat; (5) Keadilan Transisional, upaya untuk mendorong penuntasan dan akuntabilitas berbagai kejahatan terhadap HAM di masa lalu. Selama lebih dari dua dekade ELSAM telah memberikan sejumlah kontribusi dalam mendorong adopsi dan implementasi HAM di Indonesia, mulai dari pengesahan berbagai konvensi internasional HAM, hingga pembentukan sejumlah undang-undang. Berbagai undang-undang yang lahir pasca-reformasi, seperti UU Komisi Kebenaran dan Rekonsiliasi, UU Perlindungan Saksi dan Korban, dan terakhir UU Pelindungan Data Pribadi, ELSAM secara khusus terlibat dalam proses pembentukannya.

Dalam perkembangannya saat ini, ELSAM mendorong lahirnya berbagai kebijakan untuk merespons kecepatan inovasi teknologi digital. Kontribusi ELSAM untuk menghadirkan kebijakan digital yang menekankan pendekatan berpusat pada manusia (human centric approach), diakui publik dengan keluarnya ELSAM sebagai pemenang Good ID Award 2020, untuk kategori keamanan. Sebuah penghargaan global untuk individu dan organisasi masyarakat sipil, yang berkontribusi penting dalam mendorong hadirnya kebijakan digital yang baik.

ELSAM juga terlibat aktif dalam penguatan kelembagaan HAM di Indonesia, seperti Komisi Nasional HAM, Lembaga Perlindungan Saksi dan Korban, serta upaya memastikan konsistensi pelaksanaan HAM melalui dukungan dalam optimalisasi kebijakan Rencana Aksi Nasional (RAN) HAM. ELSAM juga secara terus-menerus melakukan penguatan kapasitas berbagai pemangku kepentingan dalam HAM, baik negara maupun masyarakat sipil. ELSAM menyelenggarakan kursus HAM berbagai topik untuk pembela HAM, pengacara publik, pengambil kebijakan, aparat penegak hukum, juga korporasi.

Menuju 2045, ELSAM memiliki tujuan akhir perubahan: “Masyarakat Indonesia yang berdaya, inklusif, setara, dan cakap teknologi dalam tatanan HAM dan demokrasi untuk keadilan sosial dan ekologis”. Diterjemahkan dalam Rencana Strategis 2025-2030 yang terbagi ke dalam 5 (lima) Sasaran Jangka Menengah (*Intermediate Outcome*), sebagaimana berikut ini:

1. Terbangunnya fondasi bagi aliansi politik dengan para reformis dalam institusi negara.
2. Menguatnya cara pandang kritis masyarakat sipil terhadap kebijakan dalam konteks semesta digital.
3. Tersedianya infrastruktur pengetahuan untuk menumbuhkan aktivisme HAM dalam semesta digital.
4. Berkembangnya konstituensi baru yang berperspektif HAM sebagai warga dalam semesta digital.
5. Terbangunnya narasi baru yang mendukung agenda HAM dan hak-hak korban dalam semesta digital.

Alamat:

Jl. Siaga II No. 31, Pasar Minggu, Jakarta 12510 INDONESIA Phone: (+62 21) 797 2662
Email: office@elsam.or.id Website: www.elsam.or.id

Media Sosial:

X: @elsamnews Instagram: @elsamnews Facebook: @elsamjkt
Youtube: @perkumpulanelam

