
Perang Informasi dan
Keamanan Nasional:
Disinformasi sebagai Instrumen Geopolitik
LEAKED
LEAKED
FAKE
NEWS
#HOAX
#PROPAGANDA
$AFE
Oleh Rudy C Tarumingkeng

Oleh:
Prof Ir Rudy C Tarumingkeng, PhD
Professor of Management NUP: 9903252922
Rektor, Universitas Cenderawasih, Papua (1978-1988, dan
Rektor, Kampus AGRO Manokwari sekarang Universitas Papua Manokwari)
Coordinator, CIDA/DIKTI SFU Burnaby BC Canada 1988-1991
Rektor, Universitas Kristen Krida Wacana, Jakarta (1991-2000)
Ketua Dewan Guru Besar, IPB-University, Bogor (2005-2006)
AI - Data Analyst, dan Ketua Senat Akademik, IBM-ASMI, Jakarta 2024-

---

rudyct75@gmail.com
23 Februari 2026
Bogor, Indonesia

PERANG INFORMASI DAN KEAMANAN NASIONAL: DISINFORMASI SEBAGAI INSTRUMEN GEOPOLITIK

Abstrak

Perang informasi (*information warfare*) semakin menjadi "lapisan" permanen dalam geopolitik kontemporer. Jika perang konvensional menarget wilayah dan aset fisik, maka perang informasi menarget "ruang kognitif"—yakni persepsi, emosi, identitas, dan kepercayaan publik terhadap institusi. Dalam konteks ini, disinformasi bukan sekadar "berita bohong", melainkan **instrumen strategis** untuk memengaruhi keputusan politik, melemahkan kohesi sosial, mengganggu legitimasi negara, dan membentuk narasi internasional demi kepentingan aktor negara maupun non-negara. Laporan Perserikatan Bangsa-Bangsa tentang *information integrity* menegaskan bahwa integritas informasi—akurasi, konsistensi, dan reliabilitas informasi—terancam oleh disinformasi, misinformasi, dan ujaran kebencian; ancaman ini telah menjadi isu keamanan dan hak asasi sekaligus. (Digital Library)
Esai ini menguraikan konsep kunci (misinformasi–disinformasi–malinformasi), logika geopolitik disinformasi, ekosistem taktik (bot, *microtargeting*, kebocoran data, *deepfake*), serta dampaknya pada keamanan nasional (stabilitas politik, keamanan siber, ketahanan ekonomi, dan keamanan sosial). Sejumlah contoh kasus—mulai dari

operasi pengaruh Rusia di media sosial yang didokumentasikan komite intelijen Senat AS, hingga laporan Taiwan tentang peningkatan serangan siber dan "troll army" disinformasi—digunakan untuk menunjukkan bagaimana disinformasi bekerja sebagai strategi "zona abu-abu" yang memadukan teknik informasi dan siber. (intelligence.senate.gov)
Pada bagian akhir, esai menawarkan kerangka kebijakan "ketahanan informasi nasional" yang menyeimbangkan keamanan dengan kebebasan berekspresi: pendekatan *whole-of-society*, penguatan komunikasi strategis, literasi media, transparansi platform, mekanisme *early warning*, dan tata kelola berbasis hak.

Kata kunci: perang informasi, disinformasi, FIMI, keamanan nasional, geopolitik, operasi pengaruh, ketahanan informasi, integritas informasi.

---

1) Pendahuluan: mengapa disinformasi menjadi senjata geopolitik yang "murah namun berdampak mahal"

Ada perubahan mendasar dalam cara kekuatan memengaruhi dunia. Pada masa lalu, "kekuatan" diasosiasikan dengan militer, industri, dan kontrol wilayah. Kini, kekuatan juga berarti kemampuan **mengatur arus informasi**: mengendalikan agenda publik, menggeser emosi kolektif, dan menciptakan kebingungan sehingga lawan tidak mampu membedakan fakta dari manipulasi.

Disinformasi unggul sebagai instrumen geopolitik karena tiga alasan:

Biaya rendah, jangkauan luas. Berbeda dari operasi militer, operasi disinformasi bisa dijalankan lintas batas dengan biaya relatif kecil, memanfaatkan platform yang sudah dipakai publik sehari-hari.

Plausible deniability. Pelaku dapat berlindung di balik akun anonim, *front organization*, *influencer* bayaran, atau jaringan "organik palsu" sehingga atribusi sulit dan respons politik lambat.

Efek kumulatif pada legitimasi. Disinformasi yang konsisten tidak selalu bertujuan membuat publik "percaya satu kebohongan", tetapi membuat publik **meragukan semua kebenaran**—sebuah strategi erosi kepercayaan.

NATO, misalnya, membahas "ancaman informasi" (*information threats*) dan membedakan misinformasi (tanpa niat jahat) dari disinformasi (dengan niat jahat); NATO menekankan bahwa misinformasi bisa berbahaya, tetapi disinformasi merupakan bagian penting dari ancaman informasi yang perlu ditangkal melalui pendekatan kebijakan dan komunikasi strategis. (NATO)

Dari sini terlihat bahwa disinformasi bukan isu "media" semata. Ia sudah masuk ranah **keamanan nasional**, karena menyasar prasyarat dasar negara modern: kepercayaan publik, kredibilitas institusi, dan legitimasi kebijakan.

---

2) Konsep dasar: misinformasi, disinformasi, dan malinformasi (MDM)

Agar analisis tidak kabur, kita perlu definisi yang operasional.

Misinformasi: informasi salah/keliru yang disebarkan tanpa niat mencelakakan.

Disinformasi: informasi salah/rekayasa yang sengaja dibuat untuk memanipulasi, merusak, atau menyesatkan individu/organisasi/negara.

Malinformasi: informasi yang berasal dari fakta, tetapi dipelintir, dibesar-besarkan, atau "dipotong konteksnya" sehingga menyesatkan dan menimbulkan dampak buruk.

Definisi MDM ini digunakan secara eksplisit oleh Canadian Centre for Cyber Security dan juga muncul dalam materi edukasi CISA AS. (Canadian Centre for Cyber Security)

Kenapa "malinformasi" penting? Karena era digital membuat manipulasi paling efektif sering bukan membuat kebohongan total, melainkan **membengkokkan kebenaran**: potongan video tanpa konteks, dokumen asli yang dibocorkan lalu diberi framing menyesatkan, atau data statistik benar yang dipilih selektif untuk membangun kesimpulan salah.

---

3) Dari propaganda klasik ke operasi pengaruh modern: perubahan medan perang informasi

Propaganda klasik bekerja lewat media terpusat: radio, surat kabar, televisi. Operasi pengaruh modern bekerja lewat sistem yang berbeda: **platform digital yang digerakkan algoritma**.

Tiga perubahan kunci:

Dari distribusi ke amplifikasi algoritmik. Konten tidak hanya "diterbitkan", tetapi "diangkat" oleh sistem rekomendasi yang mengejar keterlibatan (*engagement*). Konten provokatif sering mendapat keuntungan struktural.

Dari audiens massal ke *microtargeting*. Pesan dapat disesuaikan untuk segmen yang sangat spesifik—misalnya berdasarkan lokasi, identitas, preferensi politik, bahkan pola emosi.

Dari persuasi langsung ke polarisasi. Banyak operasi disinformasi tidak mempromosikan satu kandidat/ide secara terang, tetapi memperdalam konflik sosial sehingga "lawan" menjadi sibuk bertengkar di dalam negeri.

Dalam bahasa kebijakan Eropa, fenomena ini sering dikaitkan dengan **FIMI** (*foreign information manipulation and interference*): manipulasi dan intervensi informasi lintas-batas yang mengincar ruang publik negara lain. Proyek EUvsDisinfo (dipimpin East StratCom Task Force) dibangun sejak 2015 untuk mengidentifikasi dan meningkatkan kewaspadaan terhadap operasi disinformasi (terutama yang diasosiasikan dengan narasi pro-Kremlin). (EUvsDisinfo)

---

4) Logika geopolitik: apa tujuan strategis disinformasi?

Secara geopolitik, disinformasi biasanya diarahkan pada salah satu atau beberapa tujuan berikut:

4.1 Mengubah preferensi dan perilaku politik

Targetnya adalah keputusan: pilihan pemilu, dukungan kebijakan luar negeri, penerimaan proyek strategis, hingga sikap terhadap perang atau perdamaian.

4.2 Menurunkan legitimasi institusi negara

Narasi yang terus-menerus menyerang kredibilitas pemilu, pengadilan, media arus utama, atau lembaga kesehatan dapat membuat masyarakat tidak percaya mekanisme negara, dan mudah digerakkan oleh rumor.

4.3 Memecah kohesi sosial (polarization as a weapon)

Jika masyarakat terbelah, negara menjadi sibuk mengatasi konflik internal, energi politik habis untuk “perang budaya”, dan kapasitas menghadapi ancaman eksternal menurun.

4.4 Menutupi operasi lain (smokescreen)

Disinformasi dapat berfungsi sebagai tirai asap untuk menutup serangan siber, operasi intelijen, atau manuver militer. Dalam dokumen-dokumen

keamanan modern, operasi informasi sering dipandang sebagai bagian dari paket "hibrida" yang memadukan instrumen non-militer dan militer.

4.5 Menggeser narasi internasional

Dalam konflik internasional, kemenangan sering diperebutkan bukan hanya di medan tempur, tetapi di arena legitimasi global: siapa korban, siapa agresor, siapa pembela. Narasi memengaruhi sanksi, bantuan internasional, posisi organisasi multilateral, dan persepsi pasar.

---

5) Ekosistem taktik: bagaimana operasi disinformasi dijalankan? (model "rantai operasi")

Untuk memahami perang informasi sebagai proses, kita dapat memakai model "rantai operasi":

Tahap 1 — Penetapan tujuan dan *targeting*

Aktor menetapkan hasil yang diinginkan: menurunkan partisipasi pemilih, memicu protes, melemahkan dukungan pada aliansi, atau menciptakan ketidakpercayaan terhadap vaksin/anggaran/komisi pemilu.

Tahap 2 — Desain narasi (storyline)

Narasi biasanya memanfaatkan "titik lemah psikologis": ketakutan, kemarahan, rasa terancam, atau nostalgia. Malinformasi sering efektif karena menempel pada "fakta kecil" lalu dilebarkan menjadi "kesimpulan besar".

Tahap 3 — Produksi konten dan *seeding*

Konten dapat berupa teks, meme, video pendek, *fake account*, atau artikel pseudo-media. Pada era AI, produksi konten menjadi lebih murah, lebih cepat, dan bisa dipersonalisasi.

Tahap 4 — Amplifikasi (bot, troll, influencer, iklan)

Amplifikasi dapat dilakukan oleh:

akun bot/koordinasi akun palsu,

troll farm,

influencer yang disusupi atau dibayar,

iklan politik atau iklan isu (*issue ads*),

jaringan *cross-platform* (forum–TikTok–YouTube–X–WhatsApp).

Tahap 5 — *Hijacking* agenda publik (mainstreaming)

Ketika topik trending, media arus utama kadang ikut meliput, sehingga narasi memperoleh legitimasi "tidak langsung"—meski sebagai bantahan, namun tetap memperbesar jangkauan.

Tahap 6 — Eksploitasi dampak dan adaptasi

Aktor memantau data (komentar, share, polling, trending) lalu menyesuaikan pesan—seperti kampanye pemasaran, tetapi tujuan akhirnya adalah efek politik dan keamanan.

---

6) Disinformasi + siber: konvergensi serangan terhadap negara

Tren penting beberapa tahun terakhir adalah konvergensi perang informasi dan perang siber. Disinformasi dapat didukung oleh:

pencurian akun untuk menyebar narasi seolah "dari dalam",

peretasan untuk membocorkan data (lalu dipelintir),

spoofing situs berita,

serangan DDoS yang dibarengi narasi "pemerintah menutup informasi".

Laporan Taiwan mencontohkan bentuk konvergensi ini: National Security Bureau Taiwan menyebut peningkatan serangan siber dan aktivitas

"online troll army" yang menyebarkan disinformasi; laporan tersebut juga menyoroti keberadaan ribuan akun abnormal dan skala pesan disinformasi yang sangat besar. (Reuters)

Dari perspektif keamanan nasional, konvergensi ini berbahaya karena memperluas permukaan serangan: bukan hanya jaringan komputer negara, tetapi juga jaringan psikologis masyarakat.

---

7) Studi kasus naratif: disinformasi sebagai instrumen geopolitik dalam praktik

Kasus A — Operasi pengaruh Rusia dan polarisasi sosial

Komite Intelijen Senat AS merilis laporan bipartisan yang menguraikan bagaimana Rusia menggunakan media sosial untuk memengaruhi dan memperuncing polarisasi; laporan tersebut menegaskan bahwa taktik modern disinformasi yang dipakai Rusia kemudian diikuti aktor lain. (intelligence.senate.gov)
Di ranah penegakan hukum, laporan *Special Counsel* AS (Mueller Report) juga menyimpulkan Rusia melakukan operasi pengaruh melalui berbagai metode, termasuk kampanye media sosial. (Department of Justice)

Makna geopolitiknya bukan sekadar "campur tangan", tetapi logika yang lebih luas: merusak kepercayaan terhadap proses demokrasi sehingga negara lawan melemah dari dalam.

Kasus B — Ukraina: perang informasi sebagai front yang terus hidup

Dalam konflik Ukraina, perang informasi muncul sebagai bagian dari realitas hibrida: narasi, propaganda, dan klaim-klaim yang bersaing untuk mengendalikan legitimasi. Di level institusi, Ukraina memiliki Centre for Countering Disinformation (CCD) sebagai salah satu upaya menghadapi ancaman disinformasi. (cpd.gov.ua)

Di Eropa, EUvsDisinfo secara rutin menganalisis pola narasi pro-Kremlin, termasuk upaya menghapus identitas Ukraina melalui manipulasi narasi sejarah dan budaya. (EUvsDisinfo)

Dalam logika geopolitik, "memenangkan narasi" memengaruhi arus bantuan, dukungan publik, dan posisi negara ketiga.

Kasus C — Taiwan: disinformasi sebagai taktik zona abu-abu

Taiwan sering dijadikan contoh bagaimana disinformasi berfungsi sebagai tekanan geopolitik tanpa invasi. Laporan Taiwan menyebut pemanfaatan peretasan untuk menyamar sebagai warga/aktor domestik guna menyebarkan disinformasi dan memicu ketidakpercayaan pada institusi pertahanan. (nsb.gov.tw)
Analisis RAND juga membahas kemungkinan garis besar fokus operasi disinformasi Tiongkok terhadap Taiwan, termasuk segmentasi audiens dan tujuan yang berbeda. (RAND Corporation)

Di sini, disinformasi tidak berdiri sendiri; ia melengkapi tekanan diplomatik, ekonomi, dan militer—membentuk paket "koersi" bertahap.

---

8) Dampak pada keamanan nasional: empat dimensi kerentanan

Disinformasi menjadi isu keamanan nasional karena berdampak pada empat pilar:

8.1 Keamanan politik dan legitimasi demokrasi

Jika publik percaya pemilu selalu curang, pengadilan selalu dibeli, dan media selalu bohong, maka keputusan negara kehilangan legitimasi. Akibatnya: stabilitas pemerintahan menurun, ekstremisme meningkat, dan polarisasi mengeras.

8.2 Keamanan sosial: kohesi, konflik horizontal, dan kekerasan

Disinformasi dapat memicu kebencian terhadap kelompok tertentu, memperbesar konflik identitas, dan mengarah pada kekerasan. PBB menekankan integritas informasi terkait erat dengan perlindungan hak asasi dan pencegahan ujaran kebencian. (MFAIC)

8.3 Keamanan ekonomi: stabilitas pasar, investasi, dan reputasi negara

Rumor dan manipulasi informasi dapat memicu kepanikan pasar, *bank run*, atau melemahkan reputasi negara. Dalam dunia yang sangat terhubung, persepsi bisa memengaruhi biaya modal dan stabilitas nilai tukar.

8.4 Keamanan pertahanan: moral publik dan kepercayaan pada militer

Narasi yang sengaja menciptakan ketidakpercayaan pada militer, mempermalukan aparat, atau menebar rumor tentang kelemahan pertahanan dapat menurunkan daya tangkal (*deterrence*).

---

9) Arena regulasi dan "pertempuran norma": dari DSA Eropa hingga perdebatan kebebasan berpendapat

Perang informasi tidak hanya terjadi pada konten, tetapi juga pada **aturan** (norma) yang mengatur platform.

9.1 Uni Eropa: DSA dan rezim "systemic risk"

Digital Services Act (DSA) bertujuan menciptakan ruang digital yang melindungi hak warga dan menetapkan kewajiban bagi platform. (Digital Strategy)
Dalam ekosistem kebijakan Eropa, disinformasi diposisikan sebagai salah satu risiko sistemik yang perlu dinilai dan dimitigasi—terlihat juga dalam kajian akademik tentang regulasi disinformasi di bawah DSA.

(cogitatiopress.com)
Selain DSA, Komisi Eropa memiliki **Strengthened Code of Practice on Disinformation (2022)** yang menekankan langkah seperti *demonetisation* (memotong insentif iklan bagi penyebar disinformasi) dan komitmen industri untuk penguatan mitigasi. (Digital Strategy)

9.2 Amerika Serikat: perdebatan keamanan vs kebebasan berekspresi

Perdebatan paling keras sering muncul pada batas antara "counter-disinformation" dan "sensor". Misalnya, Global Engagement Center (GEC) AS—unit yang fokus pada disinformasi asing—ditutup, dan isu ini menjadi perdebatan politik yang tajam. (State Department)
Baru-baru ini Reuters juga melaporkan rencana portal "freedom.gov" yang dimaksudkan untuk melewati pembatasan konten di yurisdiksi lain, memperlihatkan gesekan norma lintas negara tentang moderasi konten. (Reuters)

Intinya: perang informasi juga perang tentang "model tata kelola internet": apakah menekankan perlindungan dari bahaya digital melalui regulasi ketat, atau menekankan kebebasan berekspresi yang luas meski risikonya meningkat.

---

10) Kerangka respons keamanan nasional: menuju "Ketahanan Informasi" (Information Resilience)

Jika disinformasi adalah instrumen geopolitik, respons negara tidak bisa hanya berupa "klarifikasi pemerintah" atau "pemblokiran". Respons yang efektif cenderung bersifat **berlapis**:

10.1 Lapisan intelijen & *early warning*

Pemetaan narasi berbahaya dan jaringan amplifikasi

Analitik lintas platform (dengan perlindungan privasi)

Koordinasi antar-lembaga: siber, intelijen, komunikasi publik, dan pemilu

10.2 Lapisan komunikasi strategis (StratCom)

Poin penting: komunikasi strategis bukan propaganda tandingan, melainkan penyediaan informasi faktual yang cepat, jelas, konsisten, dan mudah diakses—agar ruang rumor mengecil. NATO menekankan akses mudah ke fakta dan komunikasi proaktif untuk mengurangi dampak misinformasi/disinformasi. (NATO)

10.3 Lapisan masyarakat sipil: fact-checking dan jaringan kepercayaan

Pengalaman Taiwan sering dikutip sebagai "respons masyarakat" yang kuat melalui kolaborasi pemerintah–LSM–komunitas pemeriksa fakta. (Global Taiwan Institute)

10.4 Lapisan platform: transparansi dan mitigasi risiko sistemik

Pendekatan DSA dan Code of Practice memberi contoh bahwa platform dapat diminta menilai risiko sistemik dan menekan insentif ekonomi penyebar disinformasi (mis. demonetisasi). (Digital Strategy)

10.5 Lapisan pendidikan: literasi media sebagai "imunisasi sosial"

Literasi media tidak cukup mengajarkan "cek fakta", tetapi juga:

memahami bias kognitif,

mengenali manipulasi emosi,

membaca konteks,

membedakan opini, berita, dan propaganda.

---

11) Dilema etika dan hak: bagaimana mencegah perang informasi tanpa merusak demokrasi?

Tantangan terbesar kebijakan disinformasi adalah risiko *overreach*. Negara yang terlalu agresif dapat dituduh melakukan sensor; negara yang terlalu pasif menjadi korban operasi pengaruh.

Karena itu, kerangka berbasis hak biasanya menuntut:

Definisi yang jelas (apa yang disebut disinformasi dan apa yang masih termasuk perbedaan pendapat).

Prosedur akuntabel (siapa yang memutuskan, mekanisme banding).

Transparansi (publik tahu alasan tindakan, bukan hanya melihat "konten hilang").

Proporsionalitas (tindakan seimbang dengan tingkat bahaya).

Independensi (peran lembaga non-politik untuk audit).

PBB, dalam prinsip-prinsip integritas informasi, menekankan pentingnya melindungi hak asasi sambil merespons ancaman disinformasi dan ujaran kebencian. (MFAIC)

---

12) Relevansi bagi Indonesia: membangun ketahanan informasi sebagai komponen keamanan nasional

Dalam konteks Indonesia—negara besar, majemuk, demokratis, dan sangat aktif di media sosial—perang informasi memiliki risiko khusus:

Polarisasi identitas (agama, etnis, pusat-daerah) sebagai "permukaan serangan"

Hoaks yang memicu kepanikan ekonomi/keamanan

Interferensi narasi pada momen pemilu dan krisis

Kerentanan disinformasi dalam isu kesehatan, bencana, dan kebijakan publik

Kerangka yang bisa dipertimbangkan (secara konseptual) adalah **Ketahanan Informasi Nasional** berbasis 5 pilar:

Governance: koordinasi lintas lembaga, mandat jelas, SOP krisis informasi

Technology: pemantauan narasi, analitik, OSINT yang mematuhi privasi

Society: literasi media, pemberdayaan komunitas, fact-checking kolaboratif

Platform accountability: transparansi iklan politik/isu, akses data untuk riset, mitigasi bot/akun koordinatif (meniru pendekatan "risiko sistemik")

Strategic communication: kecepatan, konsistensi, dan kredibilitas komunikasi negara

Jika ini dijalankan, disinformasi tidak akan "hilang", tetapi dampaknya dapat diperkecil—seperti penyakit endemik yang dikendalikan, bukan wabah yang melumpuhkan.

Penutup: disinformasi sebagai senjata geopolitik menuntut respons yang sama strategisnya

Perang informasi adalah kompetisi atas realitas sosial. Disinformasi bekerja sebagai instrumen geopolitik karena menurunkan kapasitas lawan mengambil keputusan rasional, mengikis legitimasi negara, dan memecah kohesi masyarakat. Peta global menunjukkan berbagai aktor mempraktikkan operasi pengaruh: dari kasus yang didokumentasikan lembaga-lembaga AS terkait Rusia, hingga laporan Taiwan tentang kombinasi serangan siber dan disinformasi. (intelligence.senate.gov)

Namun, respons tidak boleh berubah menjadi pembatasan kebebasan yang merusak demokrasi. Karena itu, kebijakan paling kuat adalah kebijakan yang membangun **resiliensi**: memperkuat integritas informasi, literasi publik, transparansi platform, serta kemampuan negara berkomunikasi secara kredibel. Dalam abad ke-21, keamanan nasional tidak hanya berarti menjaga perbatasan, tetapi juga menjaga **ruang kognitif** bangsa.

Daftar Pustaka Ringkas (rujukan kunci)

Canadian Centre for Cyber Security. *How to identify misinformation, disinformation and malinformation (MDM).* (Canadian Centre for Cyber Security)

CISA (U.S.). *MDM recommendations / Disinformation Stops With You.* (CISA)

NATO. *NATO's approach to counter information threats.* (NATO)

United Nations. *Information Integrity on Digital Platforms (Policy Brief).* (Digital Library)

United Nations. *Global Principles for Information Integrity.* (MFAIC)

U.S. Senate Select Committee on Intelligence. *Bipartisan report on Russia's use of social media.* (intelligence.senate.gov)

Reuters. *Taiwan flags rise in Chinese cyberattacks, warns of "online troll army".* (Reuters)

Taiwan NSB. *China's Disinformation Dissemination Patterns in 2024 (report).* (nsb.gov.tw)

European Commission. *Digital Services Act (DSA).* (Digital Strategy)

European Commission. *2022 Strengthened Code of Practice on Disinformation.* (Digital Strategy)

EUvsDisinfo / EEAS East StratCom Task Force. *About & analysis pages.* (EUvsDisinfo)

U.S. State Department. *Global Engagement Center closed (statement page).* (State Department)

Reuters

Reuters

AP News

The Washington Post

The Verge

The Guardian

Glosarium

1) Konsep dan kerangka besar

Perang informasi (information warfare): penggunaan terencana informasi (dan gangguan informasi) untuk memperoleh keuntungan strategis—terutama dengan memengaruhi persepsi, emosi, dan keputusan publik/elite, bukan semata menghancurkan aset fisik.

Operasi pengaruh (influence operations): rangkaian tindakan komunikasi (terbuka maupun terselubung) untuk membentuk opini, sikap, dan perilaku target politik atau sosial.

Manipulasi & intervensi informasi asing (FIMI – foreign information manipulation and interference): tindakan lintas-batas yang

memanipulasi ruang informasi negara lain guna melemahkan kohesi sosial, legitimasi institusi, atau posisi geopolitik.

Ancaman informasi (information threats): kategori ancaman yang berfokus pada disinformasi sebagai tindakan bermaksud jahat; beberapa pendekatan NATO membedakan disinformasi (niat jahat) dari misinformasi (tanpa niat jahat), sambil menekankan bahwa dampak misinformasi tetap bisa merusak. (NATO)

Integritas informasi (information integrity): kualitas ekosistem informasi yang menjaga akurasi, konsistensi, keterlacakan, dan reliabilitas informasi publik; PBB membahasnya sebagai prasyarat demokrasi dan tata kelola digital. (Digital Library)

Ancaman hibrida (hybrid threats): kombinasi instrumen non-militer dan militer (mis. siber, disinformasi, sabotase, tekanan ekonomi) untuk mencapai tujuan politik tanpa eskalasi perang terbuka. (Reuters)

Zona abu-abu (grey-zone tactics): tindakan koersif di bawah ambang perang (termasuk disinformasi dan operasi siber) dengan *plausible deniability*.

Ruang kognitif: ranah psikologis-sosial tempat kepercayaan, identitas, dan interpretasi realitas publik terbentuk—sasaran utama operasi disinformasi.

2) Tipologi salah-informasi (MDM)

Misinformasi: informasi keliru yang disebarkan tanpa maksud merugikan. (Canadian Centre for Cyber Security)

Disinformasi: informasi keliru/rekayasa yang disebarkan dengan niat menipu, merusak, atau memanipulasi. (Canadian Centre for Cyber Security)

Malinformasi: informasi yang berbasis fakta, tetapi dipelintir/diambil di luar konteks sehingga menyesatkan atau menimbulkan dampak buruk. (Canadian Centre for Cyber Security)

Information disorder: istilah payung untuk fenomena mis-, dis-, dan malinformasi beserta dampak sosial-politiknya; dipopulerkan dalam kerangka Council of Europe. (First Draft)

3) Narasi, framing, dan dinamika psikologis

Narasi strategis: cerita besar yang mengaitkan fakta, nilai, dan identitas untuk membingkai "siapa benar/salah" dan "apa yang harus dilakukan".

Framing (pembingkaian): cara memilih sudut pandang dan penekanan (kata, simbol, contoh) sehingga publik menarik kesimpulan tertentu.

Agenda setting: kemampuan mengarahkan isu apa yang dianggap penting oleh publik (bukan hanya "apa yang benar").

Polarisasi: pembelahan tajam antarkelompok yang mengurangi kompromi dan memperbesar konflik; sering menjadi tujuan disinformasi karena melemahkan kohesi.

Efek "firehose of falsehood": model propaganda ber-volume tinggi, multikanal, cepat, repetitif, dan longgar terhadap konsistensi/kebenaran; RAND menjelaskan mengapa model ini efektif secara psikologis. (RAND Corporation)

Illusory truth effect (efek kebenaran semu): kecenderungan orang menganggap pernyataan berulang sebagai lebih benar—relevan dalam kampanye disinformasi yang repetitif.

4) Aktor dan ekosistem

Aktor negara (state actors): pemerintah/organ intelijen/militer yang menjalankan operasi pengaruh untuk kepentingan nasional.

Aktor non-negara: kelompok politik, organisasi, jaringan kriminal, atau *proxy* yang bertindak untuk motif ideologis/ekonomi atau sebagai perpanjangan aktor negara.

Proxy / cutout: perantara untuk menyamarkan keterlibatan aktor utama.

Troll farm / troll army: kelompok terorganisir yang memproduksi dan menyebarkan konten provokatif/menyesatkan secara masif; laporan Taiwan menyoroti pola akun abnormal dan pesan disinformasi berskala besar. (Reuters)

Content farm: operasi produksi konten cepat dan masif (sering *clickbait*), kadang dipakai untuk *laundering* narasi.

Astroturfing: penciptaan dukungan "akar rumput palsu" yang tampak organik.

5) Teknik digital dan operasional

Bot: akun otomatis yang mengunggah/menyebarkan konten untuk memperbesar jangkauan dan menciptakan ilusi popularitas.

Sockpuppet: identitas akun palsu yang dioperasikan manusia untuk menyamar sebagai warga biasa.

Coordinated inauthentic behavior (CIB): perilaku tidak autentik yang dikoordinasikan (akun palsu/jaringan akun) untuk memanipulasi percakapan publik.

Microtargeting: penargetan pesan ke segmen audiens kecil berdasarkan data perilaku/demografi; meningkatkan efisiensi persuasi dan polarisasi.

Amplifikasi algoritmik: penguatan jangkauan konten oleh sistem rekomendasi platform berbasis keterlibatan (*engagement*).

Synthetic media / deepfake: konten audio-visual sintetis (sering AI) yang meniru orang/peristiwa; berpotensi meningkatkan kredibilitas disinformasi. (Canadian Centre for Cyber Security)

Hack-and-leak: operasi membobol sistem untuk mencuri data lalu membocorkan (sering disertai framing menyesatkan).

Attribution (atribusi): penetapan pelaku/asal operasi; sulit karena anonimitas dan penggunaan *proxy*.

OSINT (open-source intelligence): pengumpulan intelijen dari sumber terbuka (media, platform, dokumen publik) untuk memantau narasi dan jaringan.

6) Tata kelola, regulasi, dan standar kebijakan

DSA (Digital Services Act): regulasi UE yang menetapkan kewajiban bagi layanan/platform online untuk menciptakan ruang digital yang lebih aman dan melindungi hak pengguna. (Digital Strategy)

Code of Practice on Disinformation (UE): kerangka komitmen industri (diperkuat 2022) untuk menekan insentif ekonomi disinformasi (mis. *demonetisation*) dan meningkatkan langkah mitigasi. (Digital Strategy)

EUvsDisinfo / East StratCom Task Force: proyek unggulan layanan diplomatik UE untuk mendeteksi, menganalisis, dan meningkatkan kewaspadaan terhadap kampanye disinformasi (dibentuk 2015). (EUvsDisinfo)

Whole-of-society approach: pendekatan ketahanan informasi yang melibatkan negara, platform, media, akademia, dan masyarakat sipil (bukan sekadar respons pemerintah).

7) Respons dan ketahanan

Debunking: membantah klaim salah dengan bukti dan konteks.

Prebunking / inoculation: "imunisasi kognitif" dengan memperkenalkan pola manipulasi sebelum publik terpapar, agar lebih tahan terhadap disinformasi.

Early warning system: mekanisme deteksi dini lonjakan narasi berbahaya dan jaringan amplifikasinya.

Komunikasi strategis (StratCom): komunikasi publik proaktif, konsisten, dan berbasis fakta untuk memperkecil ruang rumor; NATO menekankan pentingnya akses mudah ke fakta dan komunikasi proaktif. (NATO)

Ketahanan informasi (information resilience): kapasitas sistem sosial-politik untuk menyerap guncangan disinformasi tanpa kehilangan kepercayaan, kohesi, dan legitimasi.

Daftar Pustaka (pilihan inti, format APA ringkas)

A. Dokumen PBB dan prinsip global

United Nations. (2023). *Our Common Agenda: Policy Brief 8—Information Integrity on Digital Platforms (EOSG/2023/8)*. (Digital Library)

United Nations. (2024). *United Nations Global Principles for Information Integrity: Recommendations for Multi-stakeholder action*. (Digital Library)

B. NATO, UE, dan kerangka kebijakan platform

NATO. (2025, February 3). *NATO's approach to counter information threats*. (NATO)

European Commission. (n.d.). *The Digital Services Act (DSA)*. (Digital Strategy)

European Commission. (2022). *The 2022 Code of Practice on Disinformation (policy page)*. (Digital Strategy)

European Commission. (2022, June 15). *Strengthened Code of Practice on Disinformation (Press corner IP/22/3664)*. (European Commission)

European External Action Service (EEAS). (n.d.). *EUvsDisinfo (flagship project of East StratCom Task Force)*. (European External Action Service)

C. Panduan keamanan siber & ketahanan infrastruktur

Canadian Centre for Cyber Security (Communications Security Establishment). (2024). *How to identify misinformation, disinformation and malinformation (ITSAP.00.300)*. (Canadian Centre for Cyber Security)

Cybersecurity and Infrastructure Security Agency (CISA). (2022). *Protecting Critical Infrastructure from Misinformation and Disinformation—CSAC recommendations (June 2022)*. (CISA)

D. Laporan resmi & kasus operasi pengaruh

U.S. Senate Select Committee on Intelligence. (2019). *(U) The Committee's Review of Russia's Use of Social Media (Report, Volume 2)*. (intelligence.senate.gov)

Mueller, R. S., III. (2019). *Report on the Investigation into Russian Interference in the 2016 Presidential Election (Volume II)*. U.S. Department of Justice. (Department of Justice)

National Security Bureau (Taiwan). (2024). *China's Disinformation Dissemination Patterns in 2024*. (nsb.gov.tw)

Reuters. (2025, October 14). *Taiwan flags rise in Chinese cyberattacks, warns of "online troll army"*. (Reuters)

Reuters. (2026, February 18). *US plans online portal to bypass content bans in Europe and elsewhere*. (Reuters)

E. Literatur akademik/riset rujukan

Wardle, C., & Derakhshan, H. (2017). *Information Disorder: Toward an interdisciplinary framework for research and policy making*. Council of Europe. (First Draft)

Paul, C., & Matthews, M. (2016). *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*. RAND. (RAND Corporation)

Bradshaw, S., Bailey, H., & Howard, P. N. (2021). *Industrialized Disinformation: 2020 Global Inventory of Organised Social Media Manipulation (Working Paper 2021.1)*. Oxford Internet Institute. (demtech.oii.ox.ac.uk)

Harold, S. W. (2024, April). *How Would China Weaponize Disinformation Against Taiwan in a Cross-Strait Conflict?* RAND Commentary. (RAND Corporation)

F. Lembaga pemantau dan respons negara (contoh)

Center for Countering Disinformation (Ukraine). (n.d.). *Main page / institutional materials*. (cpd.gov.ua)

Copilot for this article - Chatgpt 5.2 Thinking. Access date: 23 Februari 2026. Prompting on Writer's account (Rudy C Tarumingkeng)

https://chatgpt.com/c/699c3562-9014-839c-a748-092b1404fbb4