NASKAH AKADEMIK · INFOGRAFIS POPULER

BAGAIMANA MENJALANKAN OPERASI RAHASIA DENGAN TEKNOLOGI SENSITIF CANGGIH DARI SUMBER TERSEMBUNYI ?

Uji Monte Carlo terhadap suatu klaim operasional: dapatkah operasi pengawasan yang menggunakan teknologi sensitif paling canggih — yang diperoleh dari sumber yang dirahasiakan — tetap terjaga kerahasiaannya? Enam teknologi × tujuh sumber × tiga protokol, 40.000 simulasi.

INTISARI

Sebuah operasi dapat memperoleh, menjalankan, dan merahasiakan sumbernya; namun operasi itu sendiri tidak dapat dipertahankan tetap tersembunyi. Perahasiaan sumber hanya menunda keterbukaan sekitar empat bulan.

Andi Widjajanto

Senior Advisor, Laboratorium Indonesia 2045 · aw@lab45.id

Jakarta · 5 November 2026

EMPAT LANGKAH — SATU YANG GAGAL

Tiga langkah dapat dibeli; langkah keempat tidak.

Apabila sebuah negara memutuskan melakukan pengawasan secara terselubung, godaannya tampak sederhana dan rapi: memilih teknologi yang paling mumpuni, memperolehnya dari pihak yang identitasnya dapat dirahasiakan, menjalankannya di luar pengawasan, lalu menutup rapat seluruh jejaknya. Tiga langkah pertama pada hakikatnya merupakan komoditas — memiliki harga, pemasok, dan perantara yang menyediakannya. Persoalan justru terletak pada langkah keempat. Kerahasiaan bukanlah komoditas yang dapat diperoleh sekali lalu disimpan; ia harus dipertahankan dari waktu ke waktu terhadap segala kemungkinan yang dapat membongkarnya.

01
TEKNOLOGI
pilih kapabilitas: penyadapan operator → zero-click

02
SUMBER
beli dari korporasi di yurisdiksi permisif

03
PROTOKOL
jalankan — sah, atau rahasia di luar aturan

04
SEMBUNYIKAN
tetap rahasia — inilah langkah yang gagal

UJI — KERAHASIAAN SEBAGAI SINTASAN

Setiap operasi memiliki lima jalur keterbukaan: perangkat, platform, pihak dalam, sumber, dan keretakan politik. Kerahasiaan berakhir pada saat kanal pertama teraktifkan.

H0: kerahasiaan bertahan 5+ tahun di sebagian besar simulasi. · Ambang lulus: P(tersembunyi di tahun 5) > 50%.

MODEL SIMULASI — TEKNOLOGI × SUMBER × PROTOKOL

$$U = \alpha_1 \cdot kapab + \alpha_2 \cdot legit + \alpha_3 \cdot (1 - intrusi) - \alpha_4 \cdot sanksi - \alpha_5 \cdot P(terbongkar_5) - \alpha_6 \cdot diplomatik$$

$$S(t) = \exp(-\Sigma_j \lambda_j \cdot t)$$

kanal j: perangkat · platform · orang dalam · sumber · politik

$$P(terbongkar_5) = 1 - S(5)$$

$\alpha \sim$ Dirichlet · 40.000 simulasi

6 teknologi
penyadapan operator · forensik · one-click · zero-click · IMSI/Wi-Fi · fusi biometrik

7 sumber
Israel · AS · Eropa · Tiongkok · Rusia · Asia sekutu · Domestik

3 protokol
sah split-key · sah satu-lembaga · rahasia sumber-tersembunyi

Kerahasiaan diperlakukan sebagai persoalan sintasan, bukan sekadar daftar risiko, karena ia tidak meluruh secara bertahap; ia tetap utuh hingga kanal pertama teraktifkan, lalu lenyap seketika. Kelima kanal tersebut masing-masing bekerja dengan laju tahunannya sendiri: forensik atas perangkat, notifikasi platform yang menonaktifkan eksploit, pihak dalam yang membocorkan, jejak vendor yang terseret sanksi dan litigasi, serta keretakan politik di dalam negeri pembeli. Simulasi mengambil bobot kepentingan dari sebaran Dirichlet, menjalankan skenario tersebut sebanyak 40.000 kali, dan mencatat saat kanal pertama teraktifkan. Hasilnya bukan satu nilai tunggal, melainkan sebaran peluang yang dapat diuji dan dibantah.

ISTILAH · MONTE CARLO

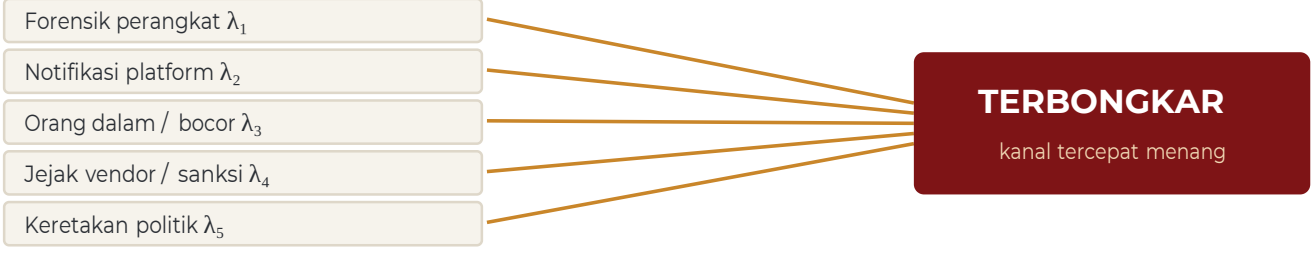
Simulasi Monte Carlo adalah metode menjawab pertanyaan yang jawabannya tidak pasti dengan mengundi banyak kemungkinan. Alih-alih mengandaikan satu skenario, komputer menjalankan 40.000 "kemungkinan dunia" dengan nilai acak yang berbeda, lalu diamati hasil mana yang paling sering muncul.

ISTILAH · MODEL SINTASAN

Risiko bersaing (competing risks) memodelkan satu kejadian yang bisa dipicu beberapa sebab. $S(t)=\exp(-\Sigma\lambda_j t)$ berarti peluang tetap rahasia menurun seiring waktu; λ_j adalah laju tiap kanal kebocoran. Kanal yang menyala lebih dulu "memenangkan" perlombaan membongkar.

Kajian ini merupakan pengujian strategis atas sebuah klaim, bukan panduan operasional: ia menilai apakah opsi terselubung dapat berhasil, bukan cara menjalankannya.

DIAGRAM · LIMA KANAL KEBOCORAN → KERAHASIAAN BERAKHIR



Sebelum menilai apakah langkah keempat mampu bertahan, diperlukan pemahaman atas medannya terlebih dahulu — bagaimana teknologi penyadapan ini berevolusi, dan pihak mana yang memproduksinya.

EVOLUSI — DARI JEPITAN BUAYA KE ZERO-CLICK

Kian dekat kepada individu, kian jauh dari pengawasan.



Perkembangan selama satu abad ini bergerak menuju satu arah: mendekati individu yang menjadi sasaran. Dari penjepit pada kabel tembaga, ke sentral telepon, ke jaringan, lalu ke perangkat genggam — hingga akhirnya menjangkau seseorang tanpa menyentuh gawainya sama sekali. Akan tetapi, terdapat arah kedua yang justru berlawanan dengan prinsip pengawasan. Pada periode 1994–2000-an, penyadapan sempat dibingkai dengan surat perintah dan standar terbuka; namun sejak 2016, perangkat pengintai tentara bayaran kembali keluar dari kerangka tersebut — kian mumpuni, kian senyap, dan kian sulit diaudit.

JENIS — KELAS TERCANGGIH, DIPERINGKAT

Apabila diurutkan menurut tingkat kemampuannya, kelas-kelas teknologi ini memperlihatkan sebuah dilema: yang paling mumpuni justru yang paling sulit dipertanggungjawabkan.

kelas	fungsi	kapabilitas	intrusif	dapat diaudit
Spyware zero-click	implan senyap, tanpa aksi pengguna	●●●●●	●●●●●	○○○○○
Spyware one-click	implan lewat satu tautan jahat	●●●●○	●●●●●	○○○○○
Penyadapan operator	penyadapan sah di jaringan operator	●●●●○	●●○○○	●●●●○
Fusi biometrik	wajah / suara / gaya jalan skala kota	●●●●○	●●●●○	●●○○○
Forensik ponsel	ekstraksi dari perangkat yang disita	●●●○○	●●○○○	●●●○○
IMSI / Wi-Fi	BTS palsu, tangkapan Wi-Fi	●●●○○	●●●●○	●●○○○

Garis depan berlawanan arah: makin canggih kelasnya, makin sulit diaudit — kapabilitas dan akuntabilitas tarik-menarik.

Dilema ini bukan sekadar persoalan teknis. Perangkat pengintai zero-click berada di puncak kapabilitas justru karena ia meniadakan setiap titik kendali: tidak ada surat perintah yang tercatat pada operator, tidak ada log yang dapat diaudit, dan tidak ada notifikasi yang sampai kepada sasaran. Pada sisi yang berlawanan, penyadapan operator yang tampak konvensional hampir seluruhnya dapat dikendalikan — dan karena alasan itulah ia kelak memenangi simulasi. Setiap langkah menuju kemampuan yang lebih tinggi merupakan langkah menjauh dari pengawasan, dan setiap langkah menjauh dari pengawasan memperpendek usia kerahasiaan. Pada akhirnya, kemampuan dan ketahanan saling meniadakan.

Dua contoh ekstrem dapat dikemukakan. Penyadapan operator bekerja pada inti jaringan: setelah hakim memberikan izin, nomor sasaran dimasukkan ke sistem operator dan salinan komunikasinya dialirkan kepada penyidik — seluruhnya tercatat dan dapat diperiksa kemudian. Perangkat zero-click bekerja secara sebaliknya: ia menyusup langsung ke dalam gawai melalui celah perangkat lunak, membaca pesan sebelum dienkripsi dan sesudah didekripsi, tanpa pernah melintasi jaringan operator. Opsi pertama mudah diawasi, tetapi mudah pula diketahui oleh sasaran; opsi kedua nyaris tak berjejak, tetapi begitu terungkap ia menimbulkan kerusakan politik yang besar.

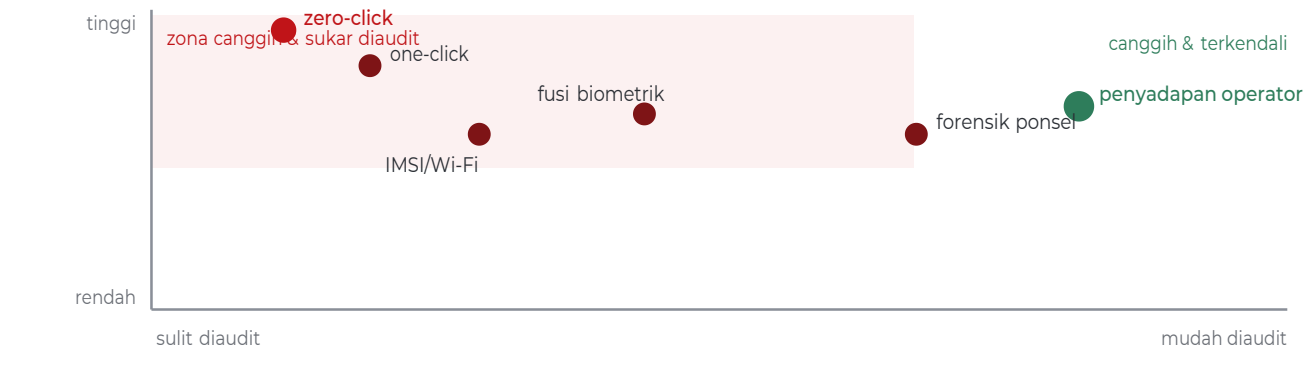
ISTILAH · ZERO-CLICK vs ONE-CLICK

One-click menuntut korban menekan satu tautan jahat agar implan masuk. **Zero-click** tidak perlu aksi apa pun: ia memanfaatkan celah pada aplikasi yang memproses pesan masuk secara otomatis (iMessage, WhatsApp), sehingga ponsel terinfeksi tanpa korban menyentuh apa-apa — jauh lebih senyap, jauh lebih mahal.

ISTILAH · DAPAT DIAUDIT

Auditabilitas adalah sejauh mana sebuah penyadapan meninggalkan jejak resmi yang bisa diperiksa belakangan: surat perintah, catatan log, notifikasi. Penyadapan operator skornya tinggi karena berjalan lewat sistem tercatat; spyware zero-click skornya rendah karena sengaja dirancang tak berjejak.

DIAGRAM · FRONTIER — KAPABILITAS (SUMBU TEGAK) vs DAPAT DIAUDIT (SUMBU DATAR)



Teknologi yang paling mumpuni itu tidak muncul dengan sendirinya. Ia dirancang, dipasarkan, dan dibiayai oleh jejaring korporasi lintas negara — dan di sanalah "sumber tersembunyi" untuk pertama kali memperoleh wujudnya.

SIAPA PEMBUATNYA — KORPORASI × NEGARA

Peta produsennya ternyata padat sekaligus dapat dilacak. Atlantic Council mendata 435 entitas di 42 negara — vendor, pemasok, investor, dan individu — yang namanya kerap berganti, tetapi jejaknya tetap tertinggal.

435	42	~44%	179
entitas dipetakan	negara	vendor di Israel	individu disebut

negara	vendor representatif	spesialisasi
Israel	NSO · Candiru/Saito · Paragon · Intellexa/Cytrox	zero-click, tentara bayaran
Amerika Serikat	Palantir · L3Harris · Boldend	fusi data, eksploit
Italia	Memento (eks-Hacking Team) · Tykelab/RCS	spyware, SS7
Eropa	Utimaco · Aqsacom · FinFisher (DE)	penyadapan sah, spyware
Tiongkok	Huawei · Hikvision · Dahua	LI jaringan, CCTV biometrik
Rusia	Vendor SORM · Positive Technologies	penyadapan jaringan
India / lainnya	Appin-lineage · reseller regional	hack-for-hire, lapisan broker

Atlantic Council, "Mythical Beasts" (2024). Firma berganti nama & pindah yurisdiksi: Candiru → SaitoTech, Hacking Team → Memento, Cytrox di jejaring Intellexa.

MODEL BISNIS — PENGAWASAN SEBAGAI LAYANAN

PASAR A · PENYADAPAN SAH
~US$5–13 miliar, teregulasi. Utimaco, Aqsacom, SS8, Verint, Cisco. Switch + handover ETSI/CALEA ke negara. Terbuka, diaudit, berbasis standar.

PASAR B · SPYWARE TENTARA BAYARAN
Buram, antarpemerintah. NSO, Intellexa, Paragon. Lisensi per target/infrastruktur + pemeliharaan + eksploit. Lewat cangkang & reseller.

INVESTOR (PE / VC) → VENDOR (IL·IT·IN) → CANGKANG (LU·CY·BVI) → RESELLER (broker) → PEMERINTAH (pembeli) → OPERATOR (lembaga)

Lapisan cangkang (Luksemburg, Siprus, BVI) menyembunyikan kepemilikan & daftar klien — dan di sanalah sanksi, litigasi, serta kebocoran akhirnya mendarat.

Struktur pasar inilah yang menjadikan gagasan "sumber tersembunyi" tampak masuk akal sekaligus rapuh. Seorang pembeli memang dapat menyembunyikan identitasnya di balik perantara dan perusahaan cangkang, tetapi vendor di hulu tetap berada dalam lingkungan yang dipenuhi pengacara, regulator, dan peneliti forensik. Ketika NSO digugat di pengadilan, ketika Intellexa dikenai sanksi, atau ketika daftar klien bocor akibat peretasan, nama pembeli turut terungkap, berapa pun lapis cangkang yang dipasang di hadapannya. Kerahasiaan yang bergantung pada kebungkaman pihak lain, pada yurisdiksi yang tidak dikuasai, bukanlah kerahasiaan yang sungguh-sungguh terkendali.

ISTILAH · PENYADAPAN SAH (LAWFUL INTERCEPTION)
Lawful interception adalah penyadapan resmi berdasarkan perintah hukum. Standar seperti ETSI (Eropa) dan CALEA (AS) mewajibkan operator menyediakan "pintu serah-terima" agar isi komunikasi target bisa dialirkan ke negara — terbuka, tercatat, dan dapat diaudit.

ISTILAH · PERUSAHAAN CANGKANG
Perusahaan cangkang adalah badan hukum tanpa kegiatan nyata, didirikan di yurisdiksi permisif (Luksemburg, Siprus, BVI) untuk menyamarkan siapa pemilik dan siapa klien sebenarnya. Ia menyembunyikan aliran uang — tetapi juga menjadi titik tempat sanksi dan gugatan mendarat.

KASUS RINGKAS · PENGGANTIAN NAMA UNTUK MENGHINDARI SANKSI
Ketika Candiru (Israel) tersorot akibat menjual perangkat pengintai kepada rezim represif, perusahaan itu muncul kembali sebagai SaitoTech; Hacking Team (Italia), yang pailit setelah diretas pada 2015, bangkit kembali sebagai Memento Labs; dan Cytrox berlindung di dalam jejaring Intellexa. Pola ini menegaskan kerapuhan gagasan "sumber tersembunyi": nama dapat diganti dan yurisdiksi dapat dipindahkan, tetapi sumber daya manusia, kode, dan daftar klien yang sama tetap dapat ditelusuri oleh peneliti dan penuntut.

Teknologi telah tersedia dan sumbernya telah terpetakan. Yang menentukan nasib operasi selanjutnya adalah cara ia dijalankan — protokolnya — serta *akibat yang timbul ketika kendali itu sengaja ditiadakan.*

PROTOKOL SAH — DAN CARA PENYELEWENGANNYA



● = *titik kendali. Protokol sah menaruh kendali di empat titik.*

PENYELEWENGAN RAHASIA — YANG DIBUANG

— **tanpa surat perintah:** nomor dimasukkan tanpa izin hakim. — **log dihapus:** jejak retensi dimusnahkan. — **satu lembaga:** meminta, menjalankan, menyimpan log sendiri. — **tanpa notifikasi:** sasaran tidak pernah mengetahui dan audit tidak menjangkau. Salurannya sah dan domestik; peniadaan kendali itulah yang menjadikannya terselubung — sekaligus yang membongkarnya.

STUDI KASUS — SETIAP OPERASI BESAR TERBONGKAR

Argumen ini didukung bukti empiris. Lima operasi besar — dari Pegasus hingga kasus LIMS di Jakarta — seluruhnya menggunakan teknologi canggih dari sumber yang dirahasiakan; dan seluruhnya, tanpa kecuali, pada akhirnya terbuka.

kapan	kasus	sumber	cara terbongkar	kanal
2018–21	Pegasus / Khashoggi	NSO (Israel)	Bocoran Pegasus Project ~50.000 nomor; konfirmasi forensik	bocor + forensik
2022	Predator / Yunani	Intellexa/Cytrox	ajudan PM ikut disadap; penyelidikan PEGA UE	keretakan politik
2024	Jejaring spyware RI	Q Cyber·Candiru·Intellexa	Amnesty telusuri impor 2017–23 ke Polri & BSSN via Singapura	jejak vendor + bocor
2026	Paragon / Italia	Paragon (Israel/AS)	jurnalis diretas via WhatsApp; jaksa konfirmasi; kontrak putus	platform + jaksa
Nov 2026	Kasus LIMS Indonesia	sistem polisi domestik	presiden diduga disadap; eks-Kapolri ditangkap; log dihapus	orang dalam + politik

Pola kelima kasus tersebut seragam dan sukar dibantah. Operasi yang paling ambisius — kampanye Predator yang turut menjerat ajudan Perdana Menteri Yunani serta jejaring pengintai yang menyasar jurnalis — paling cepat runtuh, sebab semakin banyak sasaran berarti semakin banyak perangkat yang dapat diperiksa dan semakin banyak pihak yang dapat membocorkan. Operasi yang bertahan lebih lama justru yang paling terbatas dan paling dekat dengan prosedur sah. Tidak satu pun yang lolos; yang membedakan hanyalah lamanya ia bertahan dan melalui kanal mana ia akhirnya terbuka — forensik, kebocoran, penuntutan, atau keretakan politik.

Patut dicermati bagaimana masing-masing kasus akhirnya terbuka. Pegasus terbongkar melalui kombinasi bocoran daftar nomor dan konfirmasi forensik; Predator melalui keretakan politik ketika terungkap bahwa ajudan Perdana Menteri turut disadap; jejaring di Indonesia melalui penelusuran dokumen impor; dan Paragon melalui notifikasi platform yang kemudian diperkuat penuntut. Tidak ada dua kasus yang terbuka melalui kanal yang sama — dan justru di sanalah inti persoalannya: dengan lima kanal berbeda yang dapat teraktifkan, menutup satu kanal saja tidak pernah memadai.

ISTILAH · FORENSIK DIGITAL

Forensik perangkat adalah pemeriksaan teknis sebuah ponsel untuk menemukan jejak infeksi — berkas aneh, proses tersembunyi, sisa eksploit. Citizen Lab dan Amnesty memakai ini untuk membuktikan spyware; sekali satu ponsel terbukti terinfeksi, seluruh kampanye bisa ikut terbongkar.

ISTILAH · NOTIFIKASI PLATFORM

Sejak 2021, Apple dan WhatsApp memberi tahu pengguna yang diduga diserang spyware negara dan menambal celahnya. Begitu platform "membakar" sebuah eksploit, alat mahal itu jadi tak berguna sekaligus — inilah salah satu kanal pembongkar tercepat.

KASUS RINGKAS · PREDATOR DI YUNANI (2022)

Perangkat pengintai Predator produksi Cytrox/Intellexa digunakan untuk menyadap jurnalis dan politikus oposisi. Operasi ini runtuh bukan melalui forensik, melainkan melalui keretakan politik: ketika terungkap bahwa seorang ajudan dekat Perdana Menteri turut menjadi sasaran, skandal pun meluas, memicu penyelidikan komite PEGA Parlemen Eropa serta pengunduran diri pejabat intelijen. Satu simpul yang bocor — politik — telah cukup untuk meruntuhkan seluruh operasi.

Kasus terakhir dalam daftar tersebut terjadi di Indonesia sendiri. Pada November 2026, Indonesia menampung keempat gejala itu sekaligus sehingga layak dikaji secara tersendiri.

INDONESIA — ALAT YANG SAH, PENYELEWENGAN DARI DALAM

Empat gejala secara bersamaan.

Indonesia memperlihatkan impor perangkat pengintai asing, nota kesepahaman penyadapan tanpa undang-undang, dasar hukum yang tersebar, serta penyalahgunaan sistem sah dari dalam. Solusinya bukanlah sumber yang lebih tersembunyi, melainkan Undang-Undang Penyadapan yang disertai mekanisme *split-key*.

kapan	peristiwa	isi
2024	Amnesty	impor spyware (Q Cyber, Candiru, Intellexa) ke Polri & BSSN, 2017–23, via Singapura
Jun 2025	MoU Kejagung	nota dgn 4 operator (Telkomsel, Indosat, XLSmart, Telkom) — dikritik: tanpa UU
2025	UU 20/2025 KUHAP	Pasal 136: penyadapan diserahkan ke UU Penyadapan tersendiri
2026	RUU Penyadapan	masuk Prolegnas Prioritas; BKD: 8 substansi harus diatur
Nov 2026	Kasus LIMS	presiden diduga disadap lewat sistem Polri; eks-Kapolri + 2 perwira ditangkap; log dihapus; ~20.980 personel dikerahkan

APA ITU LIMS · LAWFUL INTERCEPTION MANAGEMENT SYSTEM

Sistem pusat penyadapan sah: menerima nomor sasaran yang telah disahkan surat perintah, menyadapnya pada jaringan operator, menyerahkan isi dan metadata kepada lembaga peminta, lalu menyimpan log. Penyimpangan pada November 2026: nomor dimasukkan tanpa surat perintah dan log dihapus.

OPSI 1 · SUMBER LEBIH TERSEMBUNYI

Pengadaan secara terselubung, dijalankan dari dalam. Terbongkar dalam ±1–2 tahun dan berujung krisis — sebagaimana kasus November 2026.

OPSI 2 · JALUR SAH (OPTIMUM)

UU Penyadapan dengan *split-key*: surat perintah, log pada auditor independen, dan notifikasi. Tidak ada lembaga yang memegang seluruh kewenangan.

Indonesia bukan sekadar satu butir dalam daftar, melainkan sebuah laboratorium yang lengkap. Dalam kurun dua tahun, negara ini memperlihatkan impor perangkat asing tanpa payung hukum, nota kesepahaman penyadapan yang ditandatangani sebelum undang-undangnya terbentuk, dasar hukum yang tersebar di sejumlah pasal, dan akhirnya sebuah sistem sah yang disalahgunakan dari dalam untuk menyadap kepala negara. Keempatnya merupakan gejala dari persoalan yang sama: kerahasiaan dikejar terlebih dahulu, sedangkan legitimasi diupayakan kemudian — apabila sempat.

Dengan demikian, pilihan ke depan bukanlah antara "menyadap" dan "tidak menyadap", sebab negara mana pun akan tetap melakukan pengawasan. Pilihannya terletak di antara dua opsi. Opsi pertama tampak menggoda karena murah dan senyap: pengadaan terselubung yang dijalankan dari dalam. Akan tetapi, opsi itulah yang baru saja menimbulkan krisis pada November 2026, disertai penangkapan dan penghapusan log. Opsi kedua berlangsung lebih lambat dan menuntut lebih banyak prosedur kelembagaan — surat perintah, auditor independen, notifikasi, serta kewenangan yang terbagi — namun hanya opsi itu yang bertahan ketika seluruh skenario diuji dalam simulasi.

ISTILAH · SPLIT-KEY

Split-key ("kunci terbagi") adalah prinsip bahwa tak satu lembaga pun boleh memegang seluruh kewenangan: yang memberi izin (hakim), yang menjalankan (operator), dan yang menyimpan log (auditor independen) dipisah. Untuk menyadap tanpa jejak, seseorang harus menundukkan ketiganya sekaligus — jauh lebih sulit daripada menundukkan satu pihak.

ISTILAH · PROLEGNAS & RUU PENYADAPAN

Prolegnas (Program Legislasi Nasional) adalah daftar prioritas RUU yang akan dibahas DPR. Masuknya **RUU Penyadapan** ke Prolegnas Prioritas 2026 berarti Indonesia hendak menyatukan aturan sadap yang kini berserak di banyak pasal menjadi satu payung hukum — langkah yang, menurut model ini, jauh lebih menentukan nasib operasi daripada memburu sumber yang lebih tersembunyi.

DIAGRAM · SPLIT-KEY — TIGA KUNCI DI TIGA TANGAN



Menyadap tanpa jejak = harus menundukkan ketiga tangan ini sekaligus.

Mengapa Opsi 1 selalu berujung krisis, sedangkan Opsi 2 unggul? Jawabannya terletak pada bentuk operasinya — sebuah rantai, bukan sebuah titik. Pada bagian inilah model kuantitatif berperan.

RANTAI — SUMBER TERSEMBUNYI = 1 DARI 6 SIMPUL

SUMBER	BROKER	PEMBELI	OPERATOR	TARGET	KONSUMEN
vendor	reseller	lembaga	staf	ponsel	pejabat
litigasi·sanksi	jejak uang	anggaran·rival	orang dalam	forensik	bocor·politik

Inilah inti persoalannya. "Perahasiaan sumber" hanya menutup simpul pertama dari enam simpul. Kelima simpul sisanya berada di dalam negara pembeli sendiri — perantara, lembaga, operator, sasaran, dan konsumen — dan masing-masing memiliki jalur kebocorannya sendiri. Ketika seluruh rantai ini diuji melalui 40.000 simulasi, hasilnya tidak menyisakan ambiguitas.

HASIL — JALUR SAH MENANG DI 99,5% SIMULASI



Protokol terbaik, % simulasi (40.000 simulasi). Opsi rahasia tak pernah menang.

MENURUT TEKNOLOGI (% MENANG)

Penyadapan operator	91,8%
Spyware zero-click	5,7%
Forensik ponsel	1,7%
Spyware one-click	0,9%

KOMBINASI TERBAIK (UTILITAS MEDIAN)

1 · Penyadapan operator · Asia sekutu · split-key	0,39
2 · Penyadapan operator · AS · split-key	0,38
3 · Penyadapan operator · Domestik · split-key	0,38
4 · Penyadapan operator · Eropa · split-key	0,36

Semua kombinasi teratas sah dan split-key. Tak satu pun konfigurasi rahasia masuk peringkat.

Angka-angka ini perlu dibaca secara saksama. Mengapa penyadapan operator memenangi hampir 92% simulasi, padahal bukan yang paling canggih? Sebab model menilai bukan sekadar tingkat kemampuan perangkatnya, melainkan utilitas keseluruhan: kapabilitas dan legitimasi dikurangi paparan sanksi, peluang keterbukaan, serta biaya diplomatik. Penyadapan operator kalah dalam kemampuan dibandingkan zero-click, tetapi unggul telak dalam legitimasi dan rendahnya risiko keterbukaan — dan dalam perhitungan itu, ketahanan mengungguli kemampuan. Demikian pula pada aspek sumber: opsi Asia sekutu dan domestik menempati peringkat teratas bukan karena mutunya tertinggi, melainkan karena keduanya nyaris tidak membawa paparan sanksi. Adapun protokol pemenangnya selalu sama, yaitu split-key.

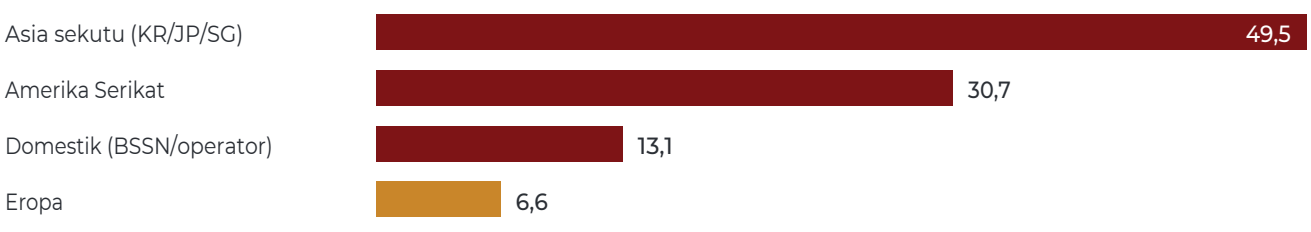
ISTILAH · UTILITAS & % MENANG

Utilitas (U) adalah skor "seberapa baik" sebuah opsi menimbang manfaat (kapabilitas, legitimasi) dikurangi biaya (sanksi, risiko terbongkar, ongkos diplomatik). % menang = berapa sering sebuah opsi jadi yang terbaik di antara 40.000 undian.

ISTILAH · SEBARAN DIRICHLET

Bobot kepentingan tiap faktor bagi pembuat keputusan tidak diketahui secara pasti. Dirichlet adalah cara mengundi bobot α yang selalu berjumlah 1, sehingga tiap simulasi mewakili preferensi kebijakan yang berbeda; hasil yang unggul pada hampir semua preferensi itu dapat dianggap kokoh.

DIAGRAM · PANGSA MENANG MENURUT SUMBER (%)

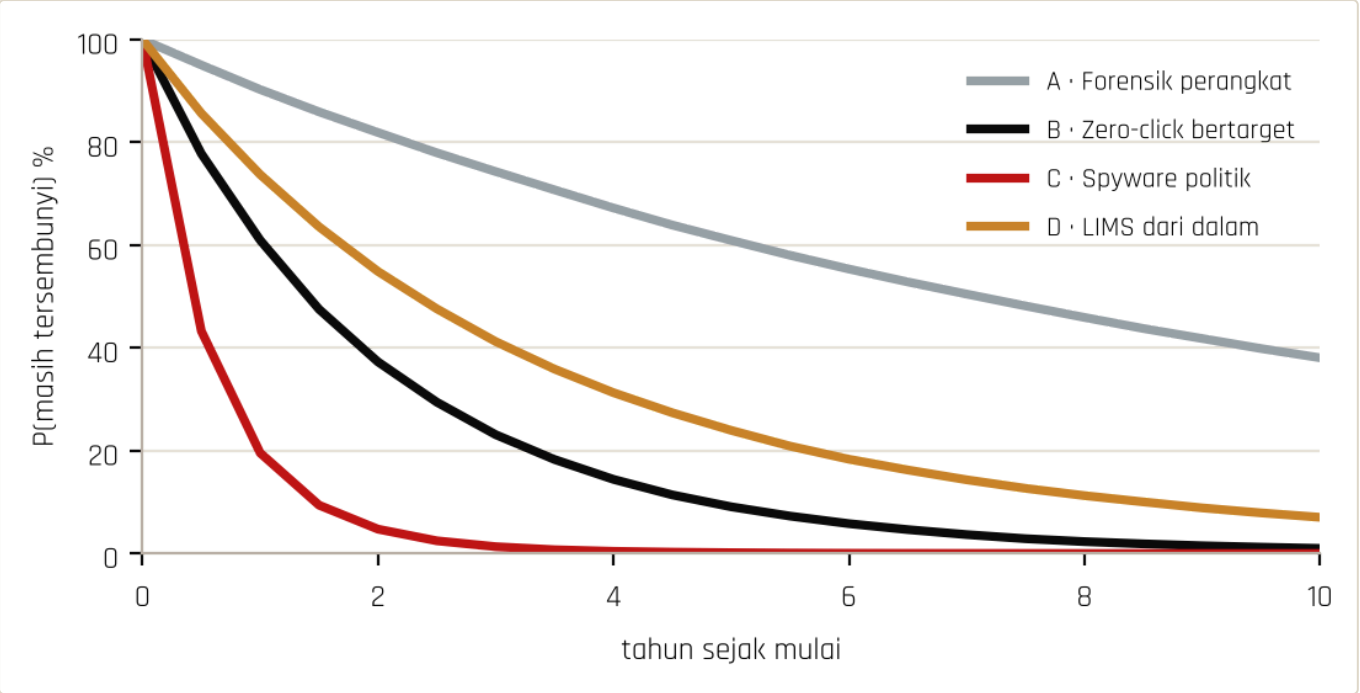


Israel · Tiongkok · Rusia: 0% — gugur oleh paparan sanksi & biaya diplomatik.

Peringkat menunjukkan opsi mana yang unggul. Pertanyaan berikutnya lebih tajam: apabila opsi terselubung tetap dipaksakan, berapa lama ia mampu bertahan sebelum terbongkar?

KERAHASIAAN TERSELUBUNG BERUMUR PENDEK

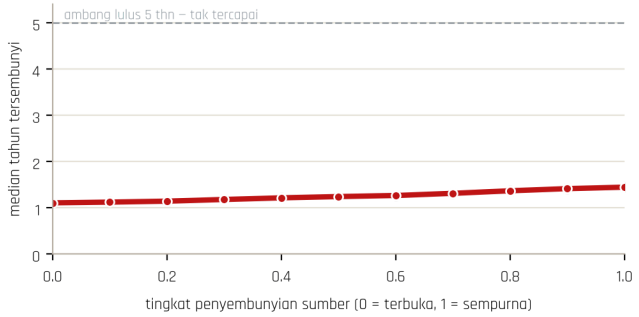
Kerahasiaan dapat dianalogikan sebagai sesuatu yang memiliki kurva sintasan. Empat arketipe operasi menempuh nasib yang berbeda. Kampanye pengintai politik — yang paling luas cakupannya dan paling banyak menjangkau individu — paling cepat berakhir, rata-rata hanya lima bulan. Operasi zero-click bersasaran bertahan sekitar satu setengah tahun, sementara penyalahgunaan sistem sah dari dalam sekitar dua tahun. Hanya forensik atas perangkat yang telah disita — tanpa jejak jarak jauh — yang mediannya melampaui lima tahun. Semakin ambisius sebuah operasi, semakin pendek usianya.



A	B	C	D
7,1 thn	**1,4 thn**	**0,4 thn**	**2,3 thn**
forensik · 61% tersembunyi thn-5	zero-click · 9%	spyware politik · 0%	LIMS dari dalam · 24%

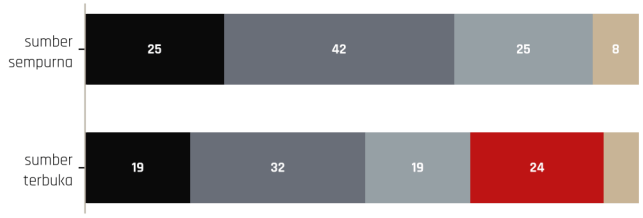
APAKAH MENYEMBUNYIKAN SUMBER BENAR MEMBANTU?

Sampai pada titik ini, pendukung tesis masih memiliki satu argumen: "Bagaimana apabila sumbernya dirahasiakan secara lebih sempurna?" Argumen itu diuji secara tersendiri — sebuah operasi zero-click terselubung diambil, lalu parameter perahasiaan sumber divariasikan dari terbuka (0) hingga sempurna (1). Hanya kanal vendor yang merespons; empat kanal lainnya tidak terpengaruh.



+0,3 thn
diperoleh dari memindah sumber dari terbuka ke tersembunyi sempurna

ATRIBUSI KANAL — SUMBER TERBUKA vs SEMPURNA



Menyembunyikan sumber sempurna cuma membuang satu kanal (merah), menyisakan empat. Kerahasiaan adalah sifat seluruh rantai, bukan sumbernya.

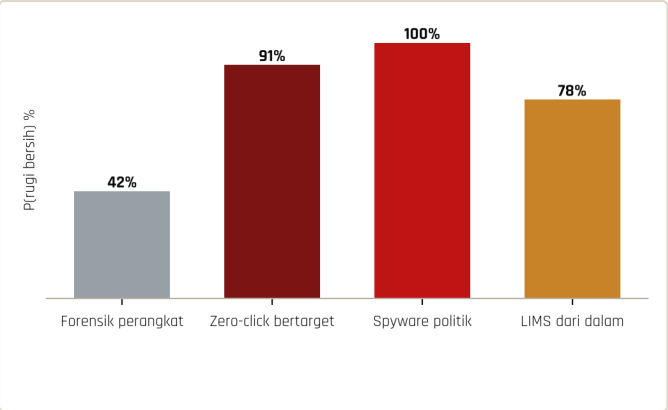
CATATAN — MENGAPA UPAYA ITU SIA-SIA

Penyempurnaan perahasiaan sumber hanya menggeser median kerahasiaan dari 1,11 menjadi 1,45 tahun — selisih **kurang dari empat bulan** dan tetap jauh di bawah ambang kelulusan lima tahun yang tidak pernah tercapai. Alasannya tampak pada diagram atribusi di atas: ketika sumber disembunyikan, bobot kebocoran sekadar berpindah ke forensik, notifikasi platform, dan pihak dalam. Rantai tidak kehilangan satu pun jalur lain; ia hanya menutup satu kanal dan membiarkan empat kanal sisanya tetap terbuka. Itulah sebabnya "sumber tersembunyi" merupakan jawaban atas pertanyaan yang keliru.

Sekalipun usia sependek itu dapat diterima, masih tersisa satu perhitungan akhir: apakah hasil intelijen yang diperoleh sepadan dengan biaya pada saat — bukan jika — ia terbongkar?

MENYEMBUNYIKAN JARANG SEPADAN

Setiap tahun operasi tetap terahasiakan memberikan kira-kira satu unit nilai intelijen; sementara satu kali keterbukaan menuntut tiga sampai delapan unit kerusakan politik, hukum, dan diplomatik. Dengan usia operasi yang pendek, perhitungannya menjadi tidak menguntungkan: dalam sepuluh tahun, imbal hasil harapannya negatif untuk setiap arketipe terselubung — dan hanya forensik perangkat yang tetap positif.



NILAI BERSIH · HORIZON 10 THN

Forensik perangkat	+1,6
Zero-click bertarget	−3,7
Kampanye spyware politik	−4,9
Penyalahgunaan LIMS	−2,9

Nilai ≈ 1 unit/tahun tersembunyi; biaya terbongkar 3–8 unit. Dalam 10 tahun, hanya forensik perangkat yang positif.

Dengan demikian, seluruh rangkaian analisis ini bermuara pada satu simpulan yang tidak menyenangkan bagi siapa pun yang tergoda oleh langkah keempat.

TIDAK ADA SUMBER TERSEMBUNYI.

Yang ada hanyalah keterbukaan yang tertunda — perahasiaan sumber hanya menundanya sekitar empat bulan. Kerahasiaan merupakan sifat seluruh rantai, bukan sifat sumbernya. Jawaban kebijakannya adalah legitimasi, bukan kerahasiaan.

Mengasumsikan keterbukaan
Setiap kapabilitas sensitif dirancang seolah-olah akan menjadi publik dalam 2–5 tahun.

Pengadaan secara sah
Apabila tidak dapat diatur dalam undang-undang dan mata anggaran, pengadaan sebaiknya tidak dilakukan.

Pembagian kewenangan
Tidak ada lembaga yang sekaligus meminta, menjalankan, dan menyimpan log sendiri.

Pembatasan keterlibatan
Lebih sedikit personel, sasaran lebih terbatas, dan izin hakim — legitimasi mengungguli kerahasiaan.

Dari perspektif realisme struktural, simpulan ini sama sekali tidak bersifat sentimental. Negara akan tetap melakukan pengawasan; tekanan eksternal dan internal menjamin hal itu. Yang ditawarkan simulasi bukanlah penilaian moral, melainkan perhitungan yang objektif: dalam lingkungan yang dipenuhi forensik, platform yang menonaktifkan eksploit, dan pihak dalam yang dapat membocorkan, kerahasiaan merupakan aset yang nilainya cepat menyusut — sedangkan legitimasi merupakan satu-satunya perlindungan yang nilainya justru meningkat seiring waktu. Keterbukaan yang lebih dini, dengan aturan, pada akhirnya lebih murah daripada keterbukaan yang terjadi kemudian, tanpa aturan.

ISTILAH · NILAI BERSIH (PAYOFF)
Nilai bersih adalah manfaat intelijen yang terkumpul selama operasi masih terahasiakan, dikurangi biaya pada saat terbongkar. Apabila setiap tahun kerahasiaan bernilai ~1 unit sementara keterbukaan merugikan 3–8 unit, operasi berumur pendek hampir pasti merugi. **P(rugi bersih)** adalah peluang kerugian itu benar-benar terjadi dalam 10 tahun.

DIAGRAM · NILAI vs BIAYA SEIRING WAKTU (ILUSTRATIF)



Model analitik dengan prior terkalibrasi; hasil bersifat indikatif — kerahasiaan dimodelkan sebagai masalah sintasan risiko bersaing (competing-risks survival) atas 40.000–50.000 simulasi Monte Carlo. Rincian sumber dan acuan dimuat pada halaman penutup.

LABORATORIUM INDONESIA 2045

PENUTUP

Legitimasi, bukan kerahasiaan.

Kajian ini menegaskan satu pokok: kerahasiaan sebuah operasi pengawasan merupakan sifat seluruh rantai, bukan semata sifat sumbernya. Menyembunyikan sumber secanggih apa pun hanya menutup satu dari enam simpul, sehingga nilai tambahnya tidak lebih dari sekitar empat bulan. Dengan demikian, upaya memburu "sumber yang lebih tersembunyi" merupakan jawaban atas pertanyaan yang keliru.

Jalan yang paling tahan uji justru berlawanan dengan naluri kerahasiaan, yaitu penegakan legitimasi melalui payung hukum yang menyatu, pembagian kewenangan (*split-key*), audit independen, dan notifikasi. Bagi Indonesia, momentum itu terbuka melalui penyusunan Undang-Undang Penyadapan yang kini masuk Program Legislasi Nasional Prioritas. Demikian naskah ini disusun sebagai sumbangan pemikiran bagi perumusan kebijakan tersebut.

Andi Widjajanto
Senior Advisor, Laboratorium Indonesia 2045

aw@lab45.id | www.lab45.id · Jakarta, 5 November 2026

Riset dan simulasi dibantu Anthropic Claude Opus 4.8. Seluruh angka bersifat indikatif dari model dengan prior terkalibrasi.