DATA CYBER INDONESIA

Ruang Riset Siber Indonesia

Efektivitas dan Batasan Operasional Alat Sadap Intelijen: Analisis Komparatif Perangkat Lunak Pegasus dan Lawful Interception Management System (LIMS)

Penulis:

Indah Dewi Sari

Indonesian cyber data research

Email: indahdewisari@datacyber.or.id

Website: https://datacyber.or.id

Tanggal Terbit: 07 November 2026

DOI: 10.5281/zenodo.24037763

Lisensi: CC BY 4.0 (Creative Commons Attribution)

Kode Verifikasi: DCY-RISET-2026-087

Efektivitas dan Batasan Operasional Alat Sadap Intelijen: Analisis Komparatif Perangkat Lunak Pegasus dan Lawful Interception Management System (LIMS)

Abstrak

Perkembangan teknologi informasi telah mengubah lanskap spionase dan penegakan hukum global. Lembaga intelijen negara saat ini bergantung pada dua doktrin utama penyadapan: intersepsi berbasis jaringan (network-level interception) dan infiltrasi berbasis perangkat (device-level infiltration). Riset independen ini bertujuan untuk menganalisis secara komparatif mekanisme kerja, efektivitas, serta batasan operasional dari dua alat sadap terkemuka, yaitu Lawful Interception Management System (LIMS) dan spyware Pegasus. Melalui metode analisis deskriptif-kualitatif berbasis literatur sekunder, riset ini menemukan bahwa LIMS unggul dalam efisiensi biaya, cakupan massal, dan kepatuhan hukum untuk menyadap jaringan telekomunikasi tradisional (suara dan SMS). Namun, adopsi enkripsi end-to-end (E2EE) pada aplikasi modern membatasi kemampuan LIMS hanya pada pengumpulan metadata. Sebaliknya, Pegasus mampu menembus batasan E2EE melalui eksploitasi Zero-Click langsung pada sistem operasi ponsel target, meskipun dengan biaya operasional yang sangat tinggi dan risiko pelanggaran hak asasi sipil yang besar. Riset ini menyimpulkan bahwa integrasi kedua sistem ini membentuk ekosistem pengawasan total, namun memerlukan regulasi pengawasan yudisial (judicial oversight) yang ketat untuk mencegah penyalahgunaan kekuasaan.

1. Latar Belakang

Keamanan nasional di era digital sangat bergantung pada kemampuan negara dalam mengumpulkan intelijen sinyal (SIGINT). Selama beberapa dekade, lembaga intelijen dan penegak hukum mengandalkan kerja sama dengan operator telekomunikasi melalui sistem terintegrasi yang dikenal sebagai LIMS. Namun, transisi masyarakat global dari SMS/telepon konvensional ke aplikasi pesan instan terenkripsi (seperti WhatsApp dan Signal) telah menciptakan fenomena "Going Dark"—kondisi di mana penegak hukum kehilangan kemampuan untuk membaca isi komunikasi target yang melintasi jaringan internet. Untuk mengatasi kebuntuan tersebut, industri spionase swasta mengembangkan military-grade spyware seperti Pegasus. Alat ini memindahkan titik sadap dari "jaringan kabel" langsung ke "dalam genggaman tangan" target. Riset ini akan membedah anatomi kerja kedua sistem tersebut untuk memahami dinamika persaingan antara privasi digital dan kebutuhan keamanan negara.

2. Rumusan Masalah

1. Bagaimana mekanisme kerja dan arsitektur teknis LIMS dalam melakukan intersepsi jaringan telekomunikasi?
2. Bagaimana anatomi kerja dan inovasi Zero-Click yang dimiliki Pegasus dalam menginfiltrasi perangkat target?
3. Bagaimana perbandingan efektivitas dan batasan operasional antara LIMS dan Pegasus dalam menghadapi tantangan enkripsi end-to-end (E2EE)?
4. Apa implikasi hukum dan rekomendasi kebijakan untuk mencegah penyalahgunaan alat sadap intelijen?

3. Tujuan

1. Menganalisis anatomi teknis LIMS sebagai metode intersepsi network-level.
2. Menganalisis mekanisme serangan Zero-Click pada Pegasus sebagai metode infiltrasi device-level.
3. Membandingkan efektivitas, biaya, dan batasan operasional kedua sistem.
4. Menyusun rekomendasi kebijakan terkait pengawasan yudisial dan pembatasan spyware komersial.

4. Batasan Masalah

Objek kajian adalah literatur sekunder terkait teknologi intersepsi dan spyware, termasuk laporan forensik digital, dokumen standar telekomunikasi, dan jurnal akademis. Riset tidak melakukan pengujian langsung atau eksploitasi perangkat. Analisis bersifat deskriptif-komparatif terhadap data yang telah dipublikasikan.

5. Tinjauan Pustaka

Riset ini menggunakan pendekatan kualitatif deskriptif dengan metode studi pustaka (literature review). Data dikumpulkan dari laporan investigasi forensik digital (seperti Citizen Lab), dokumen standar teknis telekomunikasi internasional (ETSI), serta jurnal akademis terkait keamanan siber dan hukum privasi dari periode 2020–2026. Referensi utama meliputi standar ETSI untuk LIMS, laporan The Citizen Lab mengenai exploit Pegasus, dan jurnal Journal of Cyber Policy mengenai ekosistem spyware komersial.

6. Metodologi

Riset ini menggunakan pendekatan kualitatif deskriptif dengan metode studi pustaka (literature review). Data dikumpulkan dari laporan investigasi forensik digital (seperti

Citizen Lab), dokumen standar teknis telekomunikasi internasional (ETSI), serta jurnal akademis terkait keamanan siber dan hukum privasi dari periode 2020–2026.

7. Teknik Analisis

Analisis deskriptif-komparatif terhadap literatur sekunder, meliputi pemetaan arsitektur teknis, perbandingan parameter operasional (titik intersepsi, metode serangan, kemampuan E2EE, skalabilitas, jejak forensik), dan analisis implikasi kebijakan.

8. Hasil

1. LIMS beroperasi pada lapisan infrastruktur (Core Network) operator seluler dan memisahkan data menjadi IRI (metadata) dan CC (konten).
2. LIMS unggul dalam efisiensi biaya, cakupan massal, dan kepatuhan hukum untuk menyadap jaringan tradisional.
3. LIMS gagal membaca konten saat target menggunakan enkripsi E2EE.
4. Pegasus menggunakan eksploitasi Zero-Day dan Zero-Click untuk meretas OS ponsel secara langsung.
5. Pegasus mampu menembus E2EE karena membaca data sebelum dienkripsi atau setelah didekripsi di layar ponsel.
6. Biaya lisensi Pegasus sangat mahal dan meninggalkan jejak forensik digital.
7. Integrasi LIMS dan Pegasus membentuk ekosistem pengawasan total.

9. Pembahasan

LIMS dan Pegasus mewakili dua filosofi pengawasan yang berbeda namun saling melengkapi dalam arsitektur intelijen negara modern. LIMS adalah jaring besar yang efektif untuk pemantauan massal dan pelacakan lokasi berbasis wilayah (BTS). Sementara Pegasus adalah tombak presisi yang digunakan secara khusus ketika target bernilai tinggi (high-value target) menggunakan komunikasi terenkripsi. Penyalahgunaan spyware seperti Pegasus yang tidak terkontrol dapat mengancam pilar-pilar demokrasi dan hak privasi warga negara.

10. Kesimpulan

LIMS dan Pegasus mewakili dua filosofi pengawasan yang berbeda namun saling melengkapi. LIMS efektif untuk pemantauan massal, sedangkan Pegasus adalah tombak presisi untuk target bernilai tinggi dengan komunikasi terenkripsi. Penyalahgunaan spyware tanpa kontrol dapat mengancam demokrasi dan hak privasi.

11. Rekomendasi

1. Penegakan hukum wajib mengutamakan LIMS yang memiliki jalur judicial oversight (izin pengadilan) yang jelas dan transparan.
2. Pembatasan ketat atau moratorium global terhadap pembelian military-grade spyware dari vendor swasta asing tanpa adanya mekanisme audit independen.
3. Peningkatan kesadaran keamanan siber bagi pejabat negara dan warga sipil yang rentan terhadap serangan siber tingkat tinggi.

12. Keterbatasan Riset

Penelitian ini hanya menggunakan data sekunder dari literatur yang dipublikasikan. Tidak ada pengujian langsung atau akses ke perangkat atau sistem yang dianalisis. Temuan bergantung pada akurasi dan kelengkapan laporan serta dokumen yang tersedia untuk publik.

Daftar Pustaka

1. European Telecommunications Standards Institute (ETSI). (2023). Telecommunications security; Lawful Interception (LI); Requirements for network functions. ETSI TS 101 671 V3.1.1.
2. Marczak, B., Scott-Railton, J., Al-Jizawi, S., Anstis, S., & Deibert, R. (2021). Forced Entry: NSO Group iOS Exploit Cyberweapons Deployed in the Wild. The Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto.
3. Radu, R. (2022). Stealth surveillance and the future of cybersecurity: The ecosystem of commercial spyware. Journal of Cyber Policy, 7(2), 145-162.

Halaman Verifikasi

Dokumen ini diterbitkan secara resmi oleh Data Cyber Indonesia. Pindai QR code di bawah untuk memverifikasi keaslian dokumen ini melalui website kami.

Pindai atau buka tautan berikut untuk memverifikasi:
https://datacyber.or.id/verifikasi/DCY-RISET-2026-087

Kode Verifikasi: DCY-RISET-2026-087

DOI: 10.5281/zenodo.24037763

Lisensi: CC BY 4.0

Diterbitkan oleh Data Cyber Indonesia

Tanggal: 07 November 2026