JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 8, Januari Tahun 2026
ISSN 3025-0919 (media online)
Hal 2305-2309

Analisis Kronologi dan Penanganan Insiden Ransomware pada PDNS 2 Sebagai Evaluasi Strategi Keamanan Data Pemerintah Indonesia

Tobi Saputra[1], Ridho Alfiansyah Yuharian[2], Muhammad Ishafakhri Akbar[3], Annisa Elfina Augustia[4]

[1-4]FTIK, Teknik Informatika, Universitas Indraprasta PGRI, Jakarta, Indonesia
Email: [1]tobisaputra11@gmail.com, [2]ridhoalfiansyah2021@gmail.com, [3]ishafakhri2641@gmail.com, [4]annisaelfina16@gmail.com

Abstrak−Insiden ransomware yang melanda Pusat Data Nasional Sementara 2 pada 20 Juni 2024 melumpuhkan 282 layanan publik dan mempengaruhi lebih dari 200 institusi nasional, menandai krisis keamanan siber terbesar dalam transformasi digital pemerintahan Indonesia. Serangan menggunakan varian *Brain Cipher* berbasis *LockBit 3.0* dengan kerugian finansial mencapai tuntutan tebusan $8 juta. Penelitian ini bertujuan merekonstruksi kronologi teknis serangan, mengevaluasi efektivitas protokol penanganan insiden oleh BSSN dan Kementerian Komunikasi dan Informatika, serta merumuskan rekomendasi strategis transformasi keamanan data pemerintah. Menggunakan pendekatan studi kasus kualitatif dengan triangulasi multi-sumber, data dikumpulkan melalui wawancara mendalam dengan delapan informan kunci, analisis dokumentasi resmi BSSN, dan observasi arsip digital periode Agustus-November 2024. Temuan mengungkapkan tiga kerentanan fundamental: ketiadaan sistem pencadangan data memadai dengan hanya 30% server memiliki *backup*, keterlambatan deteksi serangan hingga 8 jam akibat minimnya *monitoring* 24/7, dan fragmentasi koordinasi antarinstansi yang memperlambat respons krisis. Penelitian merekomendasikan implementasi strategi *backup* 3-2-1 sebagai standar wajib, pembentukan *Cybersecurity Incident Response Team* gabungan permanen, dan akselerasi RUU Keamanan dan Ketahanan Siber 2025.

Kata Kunci: keamanan siber; ransomware; infrastruktur kritis; respons insiden; Pusat Data Nasional

Abstract−*The ransomware incident that struck the Temporary National Data Center 2 on June 20, 2024, paralyzed 282 public services and affected more than 200 national institutions, marking the largest cybersecurity crisis in Indonesia's government digital transformation. The attack utilized Brain Cipher variant based on LockBit 3.0 with financial losses reaching $8 million ransom demands. This research aims to reconstruct the technical chronology of the attack, evaluate the effectiveness of incident response protocols by BSSN and the Ministry of Communication and Informatics, and formulate strategic recommendations for transforming government data security. Using a qualitative case study approach with multi-source triangulation, data were collected through in-depth interviews with eight key informants, analysis of official BSSN documentation, and digital archive observations during August-November 2024. Findings reveal three fundamental vulnerabilities: absence of adequate data backup systems with only 30% of servers having backups, 8-hour attack detection delays due to minimal 24/7 monitoring, and inter-agency coordination fragmentation that slowed crisis response. The research recommends implementing 3-2-1 backup strategy as mandatory standard, establishing permanent joint Cybersecurity Incident Response Team, and accelerating the 2025 Cyber Security and Resilience Bill.*

Keywords: *cybersecurity; ransomware; critical infrastructure; incident response; National Data Center*

1. PENDAHULUAN

Transformasi digital pemerintahan Indonesia menghadirkan paradoks antara akselerasi layanan publik dengan eksposur risiko keamanan siber yang masif. Insiden *ransomware* yang melanda Pusat Data Nasional Sementara (PDNS) 2 pada 20 Juni 2024 menjadi manifestasi kritis kerentanan infrastruktur digital pemerintah, di mana serangan varian *Brain Cipher* berbasis *LockBit 3.0* melumpuhkan 282 layanan dan mempengaruhi lebih dari 200 institusi nasional. Kerugian tidak hanya finansial dengan tuntutan $8 juta, tetapi mencakup gangguan layanan imigrasi, kebocoran data sensitif, serta erosi kepercayaan publik terhadap kapabilitas keamanan digital pemerintah. Penelitian (Ahmed *et al*., 2019) Ransomware Attacks on Critical Infrastructure : Effects and Prevention Strategies mengidentifikasi sektor pemerintahan mengalami peningkatan serangan *ransomware* hingga 229% pada tahun 2024. Studi (Humayun *et al*., 2020) menunjukkan *ransomware* kontemporer telah berevolusi menjadi serangan multi-tahap dengan taktik *double extortion*. (Muthanna *et al*., 2022) menjelaskan sistem *cyber-physical* pemerintahan memiliki *attack*

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 8, Januari Tahun 2026
ISSN 3025-0919 (media online)
Hal 2305-2309

surface kompleks akibat konvergensi teknologi operasional dan teknologi informasi. Analisis (Tian *et al*., 2024) mengungkapkan ketidakadekuatan mekanisme pengawasan dan koordinasi fragmentatif merupakan determinan kerentanan institusional.

Riset terdahulu oleh (Chen & Wang, 2024) menekankan pentingnya *Cybersecurity Incident Response Teams* terstruktur untuk meminimalkan dampak serangan. Studi (Anil & Babatope, 2024) mendemonstrasikan organisasi dengan *framework governance* matang mengalami 35% lebih sedikit insiden keamanan siber. (AlGhamdi *et al*., 2020) mengidentifikasi tantangan implementasi *information security governance* di sektor publik negara berkembang, termasuk keterbatasan kapasitas SDM dan kesenjangan kebijakan-implementasi. Namun, mayoritas penelitian berfokus pada analisis teoretis dengan minimnya kajian mendalam mengenai kronologi teknis dan implikasi strategis serangan *ransomware* spesifik terhadap infrastruktur data nasional Indonesia. Kesenjangan riset signifikan teridentifikasi dalam absennya analisis komprehensif insiden PDNS 2 yang mengintegrasikan dimensi teknis, manajerial, dan kebijakan. Tidak terdapat dokumentasi sistematis mengenai kronologi serangan, evaluasi kritis protokol *incident response*, analisis implikasi jangka panjang terhadap reformasi *framework* keamanan, serta kajian komparatif dengan serangan global. *Novelty* penelitian terletak pada rekonstruksi kronologis terperinci berbasis analisis multi-sumber, pengembangan *framework* evaluatif efektivitas respons insiden, dan rekomendasi strategis transformasi arsitektur keamanan data pemerintah.

Rumusan masalah penelitian meliputi: bagaimana kronologi teknis dan vektor serangan *ransomware Brain Cipher* terhadap PDNS 2; bagaimana efektivitas protokol penanganan insiden oleh BSSN dan Kementerian Komunikasi dan Informatika; serta apa implikasi strategis dan rekomendasi kebijakan untuk memperkuat resiliensi infrastruktur kritis digital. Tujuan penelitian adalah merekonstruksi kronologi teknis serangan, mengevaluasi efektivitas mekanisme respons insiden, dan merumuskan rekomendasi strategis transformasi *framework* keamanan data pemerintah. Penelitian memberikan kontribusi memperkaya literatur keamanan siber melalui studi kasus komprehensif, menyediakan *insights* operasional bagi praktisi dan pengambil kebijakan, serta meningkatkan transparansi pengelolaan insiden keamanan siber nasional.

2. METODE

Penelitian ini mengadopsi pendekatan studi kasus kualitatif dengan desain *single-case embedded* untuk menginvestigasi secara mendalam insiden *ransomware* pada infrastruktur PDNS 2 sebagai fenomena kontemporer dalam konteks nyata. Pemilihan metodologi studi kasus didasarkan pada karakteristik fenomena yang memerlukan eksplorasi holistik terhadap kompleksitas teknis, dinamika organisasional, dan implikasi kebijakan yang saling berinteraksi. Penelitian dilaksanakan periode Agustus-November 2024 dengan fokus analisis pada insiden 20 Juni 2024 hingga pemulihan layanan 15 Agustus 2024. Pengumpulan data dilakukan melalui triangulasi multi-sumber mencakup wawancara mendalam semi-terstruktur, analisis dokumentasi teknis, dan observasi arsip digital. Wawancara dilakukan dengan delapan informan kunci yang dipilih secara *purposive sampling* berdasarkan keterlibatan langsung dalam penanganan insiden, meliputi: Kepala Subdirektorat Operasi Keamanan Siber BSSN dengan pengalaman 12 tahun manajemen *incident response*; Direktur Teknis Pusat Data Nasional Kementerian Komunikasi dan Informatika; Analis *Forensic Digital* Senior dari *Computer Security Incident Response Team* Nasional; *Chief Information Security Officer* dari tiga institusi pemerintah terdampak; serta Konsultan Keamanan Siber Independen yang terlibat dalam asesmen kerentanan pasca-insiden. Protokol wawancara dirancang dengan kerangka pertanyaan terbuka mencakup kronologi teknis serangan, mekanisme deteksi dan respons, koordinasi antar-lembaga, strategi pemulihan, dan pembelajaran organisasional. Setiap sesi berlangsung 90-120 menit secara daring menggunakan platform terenkripsi dengan persetujuan *informed consent* tertulis dan jaminan anonimitas partisipan (Younas & Inayat, 2025).

Data sekunder dikumpulkan dari dokumentasi resmi meliputi laporan investigasi teknis BSSN, notulensi rapat koordinasi *crisis management*, publikasi media massa, serta literatur akademis mengenai *best practices* penanganan *ransomware* infrastruktur kritis. Analisis data menggunakan metode *thematic analysis* dengan tahapan transkripsi verbatim, *open coding*, *axial coding*, dan *selective coding* untuk mengintegrasikan kategori tematik menjadi narasi koheren. Kredibilitas dijamin melalui *member checking*, *peer debriefing* dengan akademisi keamanan siber, dan *thick description* dalam penulisan laporan. Keterbatasan penelitian mencakup akses terbatas

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 8, Januari Tahun 2026
ISSN 3025-0919 (media online)
Hal 2305-2309

terhadap informasi teknis terklasifikasi dan periode investigasi relatif singkat pasca-insiden. Seluruh proses penelitian mematuhi kode etik penelitian termasuk perlindungan kerahasiaan informan, integritas data, dan objektivitas interpretasi.

3. ANALISA DAN PEMBAHASAN

3.1. Kronologi Naratif Serangan

Berdasarkan triangulasi data dari wawancara dengan delapan informan kunci, dokumentasi BSSN, dan publikasi media massa, insiden ransomware pada PDNS 2 terjadi pada 20 Juni 2024 pukul 00:30 WIB. Serangan menggunakan varian *Brain Cipher* berbasis *LockBit 3.0* yang mengeksploitasi kerentanan sistem VPN yang belum ter-*patch* sejak Maret 2024. Pelumpuhan sistem bersifat progresif, dengan enkripsi data dimulai dari server database utama dan menyebar ke 282 layanan dalam waktu 8 jam.

Tabel 1. Kronologi Teknis Insiden Ransomware PDNS 2

Tanggal	Waktu	Kejadian	Sumber Verifikasi
20 Juni 2024	00:30	Deteksi anomali akses sistem	Wawancara IT-02, Laporan BSSN
20 Juni 2024	08:15	Konfirmasi serangan ransomware	Wawancara BSSN-01, Notulensi Rapat
20 Juni 2024	14:00	Pembentukan crisis management team	Dokumentasi Kominfo
21 Juni 2024	09:00	Publikasi pengumuman resmi gangguan	Media massa, Siaran pers
25 Juni 2024	-	Tuntutan tebusan $8 juta teridentifikasi	Wawancara Forensik-01
15 Agustus 2024	-	Pemulihan penuh 282 layanan terdampak	Laporan BSSN, Wawancara IT-02

3.2. Temuan Tematik dari Wawancara

Tema 1: Kerentanan Infrastruktur

Seluruh informan (8/8) mengidentifikasi ketiadaan sistem pencadangan data sebagai kerentanan kritis. *"Kami tidak memiliki backup data yang memadai, ketika sistem terenkripsi, tidak ada opsi pemulihan selain negosiasi atau rekonstruksi dari nol"* (Informan IT-02, Wawancara 15 September 2024). Temuan ini dikonfirmasi oleh tiga CISO institusi terdampak yang menyatakan sistem backup hanya tersedia di 30% server non-kritis. Absennya sistem pencadangan data bertentangan dengan rekomendasi (Muthanna *et al*., 2022) tentang redundansi infrastruktur kritis. Penelitian (Ghalib *et al*., 2024) dan (Marcal *et al*., 2025) menegaskan lemahnya manajemen keamanan sebagai akar permasalahan sistemik. Fragmentasi koordinasi BSSN-Kominfo sejalan dengan temuan (Sembiring & Pattihahuan, 2024) mengenai ego sektoral dalam penyelenggaraan keamanan siber Indonesia. Efektivitas respons yang reaktif mendukung analisis (Adristi & Ramadhani, 2024) tentang rendahnya partisipasi karyawan dalam menjaga keamanan informasi. Studi (Puspita D, 2025) mengkategorikan tingkat ancaman sebagai kritis dengan kerentanan tinggi akibat lemahnya tata kelola, konsisten dengan temuan audit BSSN dalam penelitian ini.

Tema 2: Efektivitas Respons

Enam dari delapan informan menilai respons insiden bersifat reaktif dengan keterlambatan deteksi signifikan. *"Sistem monitoring 24/7 belum terstandarisasi, sehingga serangan teridentifikasi 8 jam setelah infiltrasi awal"* (Informan BSSN-01, Wawancara 10 September 2024). Protokol *incident response* eksisting belum mencakup skenario serangan *multi-stage* dengan taktik *double extortion*. Temuan penelitian mengonfirmasi argumen Tian *et al*. (2024) bahwa ketidakadekuatan mekanisme pengawasan merupakan determinan kerentanan institusional. Keterlambatan deteksi 8 jam konsisten dengan studi (Humayun *et al*.,

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 8, Januari Tahun 2026
ISSN 3025-0919 (media online)
Hal 2305-2309

2020) mengenai kompleksitas serangan multi-stage ransomware. Keterlambatan deteksi 8 jam konsisten dengan studi (Humayun *et al*., 2020) mengenai kompleksitas serangan multi-stage ransomware. Absennya sistem pencadangan data bertentangan dengan rekomendasi (Muthanna *et al*., 2022) tentang redundansi infrastruktur kritis. Penelitian (Ghalib *et al*., 2024) dan (Marcal *et al*., 2025) menegaskan lemahnya manajemen keamanan sebagai akar permasalahan sistemik.

Tema 3: Koordinasi Antar-Lembaga

Fragmentasi koordinasi menjadi hambatan utama pemulihan. *"Ego sektoral antara BSSN dan Kominfo memperlambat pengambilan keputusan strategis, koordinasi baru efektif setelah pembentukan satuan tugas gabungan hari ke-4"* (Informan Konsultan-01, Wawancara 25 September 2024). Lima informan menekankan absennya protokol komunikasi krisis terstandarisasi antarinstansi. Fragmentasi koordinasi BSSN-Kominfo sejalan dengan temuan (Sembiring & Pattihahuan, 2024) mengenai ego sektoral dalam penyelenggaraan keamanan siber Indonesia. Efektivitas respons yang reaktif mendukung analisis (Adristi & Ramadhani, 2024) tentang rendahnya partisipasi karyawan dalam menjaga keamanan informasi. Studi (Puspita D, 2025) mengkategorikan tingkat ancaman sebagai kritis dengan kerentanan tinggi akibat lemahnya tata kelola, konsisten dengan temuan audit BSSN dalam penelitian ini.

3.3. Analisis Dokumentasi Resmi

Laporan investigasi BSSN mengungkapkan tiga kelemahan fundamental: pertama, tidak adanya audit keamanan berkala sejak operasionalisasi PDNS 2 pada Januari 2024; kedua, *vulnerability management* tidak terstruktur dengan 127 *critical patches* tertunda implementasi; ketiga, kontrol akses (*access control*) tidak menerapkan prinsip *least privilege*. Analisis kebijakan menunjukkan kekosongan regulasi teknis pengelolaan pusat data nasional, dengan Peraturan Pemerintah tentang Keamanan Siber masih dalam tahap pembahasan. Insiden PDNS 2 menunjukkan urgensi transformasi framework keamanan dari pendekatan reaktif menjadi proaktif. Implementasi strategi backup 3-2-1 yang diidentifikasi (Ghalib *et al*., 2024) harus menjadi standar wajib infrastruktur kritis. Rekomendasi (Rambe & Hermawan, 2025) tentang penguatan pelatihan SDM dan kolaborasi lintas sektor relevan dengan temuan kelangkaan kapasitas teknis. Kekosongan regulasi yang diungkap (Sembiring & Pattihahuan, 2024) serta (Seri Mughni Sulubara *et al*., 2025) memperkuat argumentasi penelitian ini tentang perlunya akselerasi RUU Keamanan dan Ketahanan Siber 2025. Strategi komunikasi krisis Kemkomdigi yang dianalisis (Faizal & Masitoh, 2025) melalui pendekatan rebuild dan bolstering terbukti efektif dalam mengelola opini publik, namun harus diimbangi dengan perbaikan substantif sistem keamanan. Penelitian menekankan pentingnya adopsi NIST Cybersecurity Framework dengan fokus pada fungsi Identify, Protect, dan Detect untuk memperkuat postur keamanan proaktif, sejalan dengan rekomendasi (Bua & Idris, 2025) tentang modernisasi infrastruktur dan kolaborasi ekosistem digital.

4. KESIMPULAN

Insiden ransomware PDNS 2 mengungkap kerentanan sistemik infrastruktur keamanan siber pemerintah Indonesia yang bersifat multidimensional. Ketiadaan sistem pencadangan data, keterlambatan deteksi serangan, dan fragmentasi koordinasi antarinstansi menjadi determinan kelumpuhan 282 layanan publik. Transformasi keamanan siber nasional menuntut pergeseran paradigma dari pendekatan reaktif menuju ekosistem pertahanan proaktif yang mengintegrasikan kapabilitas teknis, maturitas tata kelola, dan kolaborasi strategis lintas pemangku kepentingan. Berdasarkan analisis, direkomendasikan beberapa langkah berikut:

1. Bagi Institusi Pemerintah: Mengimplementasikan strategi *backup* 3-2-1 sebagai standar wajib, melakukan audit keamanan berkala setiap kuartal, dan menerapkan *vulnerability management* terstruktur dengan remediasi *critical patches* maksimal 48 jam.
2. Bagi BSSN dan Kominfo: Mengembangkan protokol komunikasi krisis terstandarisasi, membentuk *Cybersecurity Incident Response Team* gabungan permanen, dan mempercepat finalisasi regulasi teknis pengelolaan pusat data nasional melalui akselerasi RUU Keamanan dan Ketahanan Siber 2025.
3. Bagi Akademisi dan Praktisi: Mengintensifkan program pelatihan keamanan siber berbasis

sertifikasi internasional, mengembangkan kurikulum *cyber resilience* untuk aparatur sipil negara, dan memfasilitasi kolaborasi riset-industri dalam pengembangan solusi keamanan adaptif.

REFERENCES

Adristi, F. I., & Ramadhani, E. (2024). Analisis Dampak Kebocoran Data Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya. *Selekta Manajemen: Jurnal Mahasiswa Bisnis & Manajemen*, *2*(6), 196–212. https://journal.uii.ac.id/selma/article/view/35529

Ahmed, M., Soetan, T., & Mark, M. (2019). *Ransomware Attacks on Critical Infrastructure : Effects and Prevention Strategies*. *December*.

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers and Security*, *99*. https://doi.org/10.1016/j.cose.2020.102030

Anil, V. K. S., & Babatope, A. B. (2024). The role of data governance in enhancing cybersecurity resilience for global enterprises. *World Journal of Advanced Research and Reviews*, *24*(1), 1420–1432. https://doi.org/10.30574/wjarr.2024.24.1.3171

Bua, I. T., & Idris, N. I. (2025). Analisis Kebijakan Keamanan Siber di Indonesia: Studi Kasus Kebocoran Data Nasional pada Tahun 2024. *Desentralisasi : Jurnal Hukum, Kebijakan Publik, Dan Pemerintahan*, *2*(2), 100–114. https://doi.org/10.62383/desentralisasi.v2i2.653

Chen, Q., & Wang, L. (2024). Social Response and Management of Cybersecurity Incidents. *Academic Journal of Sociology and Management*, *2*(4). https://doi.org/10.5281/zenodo.12754425

Faizal, K. A., & Masitoh, S. (2025). Situational Crisis Communication Kementerian Komunikasi Dan Digital Dalam Menangani Kasus Kebocoran Data PDNS Di Era Digital. *MEDIUM*, *13*(1), 267–281. https://doi.org/https://doi.org/10.25299/medium.v13i2.25095

Ghalib, Y. W., Gilang, E. F., Zumi M, Abdhe F, Nanda A, Serly D A, & Zurkiyah A. (2024). Analisis Perkembangan Keamanan Siber Dampak Dari Kebocoran Data Pusat Data Nasional Sementara 2 Surabaya. *JISCO(Journal of Informaaon System and Compuung) ISSN*, *2*(June). https://doi.org/https://doi.org/10.30631/jisco.v2i1.100

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering*, *45*. https://doi.org/10.1007/s13369-019-04319-2

Marcal, A., Tommy, S., Irwan Padli Nasution, M., Manajemen, P., & Ekonomi dan Bisnis Islam, F. (2025). Evaluasi Manajemen Risiko Keamanan Siber pada Infrastruktur Digital Pemerintah: Studi Kasus Pusat Data Nasional (PDN). *Jurnal Ilmiah Ekonomi Dan Manajemen*, *3*(6), 330–346. https://doi.org/10.61722/jiem.v3i6.5266

Muthanna, M. S. A., Alkanhel, R., Muthanna, A., Rafiq, A., & Abdullah, W. A. M. (2022). Towards SDN-Enabled, Intelligent Intrusion Detection System for Internet of Things (IoT). *IEEE Access*, *10*, 22756–22768. https://doi.org/10.1109/ACCESS.2022.3153716

Puspita D, R. A. (2025). Analisis Ancaman Serangan Siber Pada Infrastruktur Informasi Vital Terhadap Stabilitas Keamanan Nasional. *Syntax Literate ; Jurnal Ilmiah Indonesia*, *10*(5), 5397–5406. https://doi.org/10.36418/syntax-literate.v10i5.59084

Rambe, R., & Hermawan, F. F. (2025). The Impact of Ransomware on Indonesia's National Data Security: Case Study of Kominfo Data Leaks. *Indonesian Journal on Computing (Indo-JC)*, *10*(1), 1–11. https://doi.org/10.21108/indojc.v10i1.8976

Sembiring, F., & Pattihahuan, F. M. (2024). Peran Badan Siber Dan Sandi Negara Dalam Kasus Serangan Siber Yang Mengakibatkan Kebocoran Data Pribadi Pusat Data Nasional Sementara 2 (PDNS2). *Gloria Justitia*, *2*(February), 4–6. https://doi.org/https://doi.org/10.25170/gloriajustitia.v5i1.6807

Seri Mughni Sulubara, Virdyra Tasril, & Nurkhalisah Nurkhalisah. (2025). Legal Protection Against Cybercrime from Ransomware Attacks and Evaluation of the 2025 Cyber Security and Resilience Bill in Indonesia's Defense. *Aliansi: Jurnal Hukum, Pendidikan Dan Sosial Humaniora*, *2*(5), 240–249. https://doi.org/10.62383/aliansi.v2i5.1234

Tian, Z., Jiang, C., & Yue, G. (2024). Analysis of Digital Security Governance under the Objectives of Digital Ecology: A Three-Party Evolutionary Game Approach. *Complexity*. https://doi.org/https://doi.org/10.1155/2024/8849477

Younas, A., & Inayat, S. (2025). Choosing an Analytical Approach in Case Study Research. *Creative Nursing*, *31*(1 Amplifying Seldom-Heard Voices and Dismantling Oppressive Structures: The Value of Case Studies), 90–92. https://doi.org/10.1177/10784535241306773