Columbia University
School of International and Public Affairs

The Operational Honeypot Mirror for Adversary Disruption (OHMAD): A Proactive Defense Model for Pipeline Ransomware

Rameen Dhindsa
Anna Marchese
Nasak Pongsri
Arnav Sahai
Diana Slobodian
Melinda Xia

INAFU6518: Cybersecurity: Technology, Policy, & Law
Professors Jason Healey, Charles Carmakal, Evan Wolff

December 2025

Introduction

Ransomware attacks on U.S. critical infrastructure have exposed a persistent strategic imbalance: attackers move first and learn quickly, while defenders react late and in isolation. To give the private pipeline sector the upper hand, this paper proposes the Operational Honeypot Mirror for Adversary Disruption (OHMAD) — a sector-led deception system that offers early warning, actionable intelligence, and coordinated disruption capabilities. Instead of waiting for attackers to breach live systems, OHMAD draws them into a high-fidelity mirror network designed to capture their activities and infrastructure. This comes at a moment when the federal government is increasing reliance on private firms to shoulder frontline responsibility for cyber defense and disruption.[1]

The paper proceeds as follows: Section I describes the asymmetries revealed by the Colonial Pipeline attack; Section II introduces OHMAD and explains how deception reverses these asymmetries; Section III details its technical architecture; Section IV outlines OHMAD's governance and sustainability; Section V examines legal and regulatory conditions for its deployment; and Section VI assesses impact, risk, and potential expansion to other critical infrastructure sectors.

I. The Problem: Ransomware Asymmetry and the Colonial Pipeline Failure

On May 7th, 2021, the Russian ransomware group DarkSide infiltrated Colonial Pipeline, the largest refined products pipeline in the US. The pipeline spans over 5,500 miles and supplies 45% of the East Coast's fuel, providing energy for over 50 million people.[2] DarkSide gained access via a legacy virtual private network (VPN) account that lacked multi-factor authentication (MFA), using a password that was exposed after a third-party data breach. Within two hours, the group had exfiltrated 100 GB of sensitive data and encrypted Colonial's Information Technology (IT) systems (e.g., billing and accounting). Although Colonial's Operational Technology (OT) systems were not directly impacted, the company shut down pipeline operations for five days as a precaution.

Three asymmetries worked in DarkSide's favor: speed, opacity, and financial leverage. Darkside worked faster than defenders could detect or patch, concealed its tooling until after the breach, and leveraged Colonial's stolen data to demand a ransom payment under extreme time pressure.

U.S. cybersecurity policy at the time of the attack emphasized reporting and recovery, rather than preemptive disruption. Ransomware attacks across the nation more than doubled between 2019

[1] Jamie Tarabay, "Trump Administration Turning to Private Firms in Cyber Offensive," *Yahoo Finance*, December 12, 2025, https://finance.yahoo.com/news/trump-administration-turning-private-firms-191259484.html

[2] Brian Fung and Geneva Sands, "Colonial Pipeline CEO Tells Congress Company Did Not Have Backup Plan Before Ransomware Attack," CNN, June 8, 2021, https://www.cnn.com/2021/06/08/politics/colonial-pipeline-ceo-on-capitol-hill-ransomware

and 2020, while TSA guidance for pipelines remained voluntary and unenforceable.[3] The government's hands-off approach meant that cybersecurity implementation was in the hands of the private sector, which operates 85% of the nation's critical infrastructure.[4]

Even with a $40 million annual cybersecurity budget, Colonial fell to a single overlooked password, causing massive fuel shortages ahead of Mother's Day weekend.[5] This cost Colonial over $1.2 billion in lost productivity, including a $4.3 million ransom payment. The incident revealed a hard truth: critical infrastructure is not failing due to complex zero-days. It is failing because threat actors exploit everyday weaknesses faster than defenders can identify or respond to them. With over 2.8 million miles of natural gas and hazardous liquid pipelines across the country, owned and operated by over 3,000 private companies, this vulnerability is systemic.[6]

II. The Solution: The Operational Honeypot Mirror for Adversary Disruption (OHMAD)

To pre-empt ransomware attacks against the private pipeline sector, this paper proposes OHMAD — the Operational Honeypot Mirror for Adversary Disruption — a deception system offering pipeline operators a shared breach intelligence and disruption layer to their existing cybersecurity systems. OHMAD presents attackers with a convincing but false target: a high-fidelity mirror of pipeline IT and OT systems intentionally exposed in the same manner as known vulnerabilities within private pipeline networks. Attackers can authenticate, conduct reconnaissance, move laterally, and deploy ransomware without touching real infrastructure, while defenders observe their every action in a controlled environment.

OHMAD counters the abovementioned asymmetries that DarkSide leveraged against Colonial. It collapses attacker speed advantages with early detection, eliminates their opacity by capturing tools and behavior in real time, and neutralizes financial leverage by extracting and sharing ransom wallet addresses with federal partners for potential seizure.

III. Architecture of Deception: The Technical Layers of OHMAD

OHMAD contains four integrated phases: 1) mirror blueprinting and construction, 2) instrumented observation, 3) multi-pillar disruption, and 4) continuous AI-driven improvements.

Phase 1: Blueprinting and Construction

---

[3] Gerrit De Vynck, Rachel Lerman, Ellen Nakashima, and Chris Alcantara, "The Anatomy of a Ransomware Attack," The Washington Post, July 9, 2021, December 13, 2025, https://www.washingtonpost.com/technology/2021/07/09/how-ransomware-attack-works/

[4] David E. Sanger and Nicole Perlroth, "White House Warns Companies to Act Now on Ransomware Defenses," The New York Times, June 3, 2021, December 13, 2025, https://www.nytimes.com/2021/06/03/us/politics/ransomware-cybersecurity-infrastructure.html

[5] "Colonial Pipeline CEO Testifies about Cyberattack at Senate Hearing," YouTube video, uploaded June 8, 2021, accessed December 13, 2025, https://www.youtube.com/watch?v=KVvvGO3mFjs

[6] David P. Pekoske, "Pipeline Cybersecurity: Protecting Critical Infrastructure," testimony before the Senate Committee on Commerce, Science, and Transportation, July 27, 2021, Transportation Security Administration, https://www.tsa.gov/news/press/testimony/2021/07/27/pipeline-cybersecurity-protecting-critical-infrastructure

OHMAD operators begin by building a decoy environment that resembles real pipeline architectures, replicating sector-specific weaknesses ransomware affiliates have exploited, like legacy VPNs without MFA, misconfigured directory environments, and expired Windows Server systems.[7]

The environment includes realistic IT artifacts such as synthetic billing records, administrator credentials, personnel directories, and network diagrams designed to be internally consistent, allowing attackers to validate their access without raising suspicion. A non-functional OT simulation layer increases the mirror's realism, mimicking DNP3 and Modbus traffic,[8] SCADA polling routines,[9] and HMI-like interfaces. No real industrial equipment connects to the mirror, but these signals will appear authentic enough to convince intruders they have reached a live target, extending their dwell time within the decoy. Where available, OHMAD operators seed the mirror with stolen credentials obtained from dark-web markets. As ransomware groups routinely test such credentials against exposed enterprise systems, such credentials serve as an effective lure, drawing in threat actors actively targeting the pipeline.[10]

Phase 2: Instrumentation and Real-Time Observation

Once attackers enter the mirror, OHMAD records everything. Endpoint detection and response tools monitor the simulated IT and OT assets, producing a comprehensive record of intruder behavior. As the mirror has no legitimate users, all activity is malicious by definition, eliminating false positives that burden traditional security operations centers (SOCs).[11] OHMAD automatically extracts actionable intelligence, including adversary malware signatures, cryptographic methods, command-and-control (C2) infrastructure, privilege escalation techniques, file and encryption changes, and ransom wallet addresses, which feed directly into disruption workflows.

Phase 3: Multi-Pillar Disruption

OHMAD turns the intelligence collected in the deception environment into disruption across four pillars of former FBI Cyber Division Assistant Director Bryan Vorndran's ransomware-disruption framework: malware, infrastructure, communication, and payment.[12]

---

[7] Microsoft, *Microsoft Digital Defense Report 2025*, 2025, https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf; "Advisory AA21-076A: TrickBot Malware," *U.S. Cybersecurity and Infrastructure Security Agency (CISA)*, March 17, 2021, https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-076a

[8] DNP3 (Distributed Network Protocol) and Modbus are common industrial communication protocols in pipeline systems that carry control commands and telemetry between field devices (i.e. sensors and/or remote terminal units). In Todd Walden and Steve Hill, "A Simple Solution for More Secure Pipelines," *Emerson Automation Experts*, January 3, 2023, https://www.emersonautomationexperts.com/2023/control-safety-systems/a-simple-solution-for-more-secure-pipelines/

[9] SCADA (Supervisory Control and Data Acquisition) systems retrieve status updates from field devices (e.g. valve states and pressure levels). In *Ibid.*

[10] Palo Alto Networks Unit 42, "Extortion and Ransomware Trends January-March 2025," *Unit 42*, April 23, 2025, https://unit42.paloaltonetworks.com/2025-ransomware-extortion-trends/

[11] Amir Javadpour, Forough Jaʿfari, Tarik Taleb, Mohammad Shojafar, and Chafika Benzaïd, "A Comprehensive Survey on Cyber Deception Techniques to Improve Honeypot Performance," *Computers & Security* 140 (2024): 103792, https://doi.org/10.1016/j.cose.2024.103792

[12] Bryan A. Vorndran, "Ransomware: Attacks and Defenses," statement before the Senate Committee on the Judiciary, Washington, DC, July 26, 2021. https://www.judiciary.senate.gov/download/bryan-vorndran-727-testimony?download=1

Testifying before Congress in 2022, Vorndran emphasized that effective disruption requires imposing risks and consequences across the entire criminal enterprise, rather than targeting individual actors in isolation.[13] OHMAD adheres to this logic. Once the system captures an adversary's tools and behavior, it activates coordinated disruption measures that operate simultaneously.

Malware Pillar: Immunizing the Sector

When OHMAD captures a ransomware payload or reconnaissance tool, operators immediately extract the malware's signatures, behaviors, and Indicators of Compromise (IOCs). IOCs, including artifacts such as file hashes and registry keys that identify malicious activity, are validated, packaged, and pushed immediately to relevant Information Sharing and Analysis Centers (ISACs) — sector-specific organizations that facilitate threat data exchange — as well as to major endpoint detection and response (EDR) vendors.

Infrastructure Pillar: Identifying and Neutralizing C2 Servers

Once C2 hosts, malicious domains, and IP addresses are identified through mirror telemetry, OHMAD operators coordinate with Internet Service Providers (ISPs), cloud hosting companies, and domain registrars that can "sinkhole" these endpoints — redirecting their traffic to controlled servers for analysis — or disable them entirely. By degrading the adversary's infrastructure, this pillar increases their operational costs and forces them to constantly rebuild their networks.

Communication Pillar: Mapping Affiliate Behavior and Attribution

Threat actors reveal far more than malware and infrastructure when they operate inside OHMAD. These behaviors may help identify particular ransomware groups. OHMAD operators can communicate these unique signatures to the FBI and DOJ, improving the evidentiary basis for attribution, indictments, or sanctions.

Financial Pillar: Seizing Cryptocurrency Before Attackers Can Collect

Finally, OHMAD operators immediately relay ransom wallet information to the Department of Justice and blockchain intelligence firms like Chainalysis and TRM Labs to trace the flow of illicit funds, steps which facilitate speedy tracing and potential seizure of the funds before adversaries can collect. The post-Colonial retrieval of $2.3 million in Bitcoin demonstrated the viability of this approach.[14] OHMAD aims to make such seizures the norm rather than the exception.

Phase 4: Continuous Evolution and AI-Driven Fidelity

---

[13] Bryan A. Vorndran, "Oversight of the Federal Bureau of Investigation, Cyber Division," statement before the House Committee on the Judiciary, Washington, DC, March 29, 2022. https://docs.house.gov/meetings/JU/JU00/20220329/114533/HHRG-117-JU00-Wstate-VorndranB-20220329.pdf

[14] U.S. Department of Justice, "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists DarkSide," press release, June 7, 2021, https://www.justice.gov/archives/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

Ransomware groups update their tools and tradecraft quickly, and any static mirror will lose credibility over time. OHMAD responds by maintaining a "living" deception environment, integrating artificial intelligence (AI) components that regularly refine the mirror's fidelity.[15]

OHMAD embeds AI as a core component of its lifecycle in four ways. Agentic AI "red teams" attack the mirror to test defenses.[16] These agents probe the mirror using known Tactics, Techniques, and Procedures (TTPs) to spot weak deception signals or unrealistic configurations that might alert a human attacker. Automated vulnerability and configuration updates ensure the environment's attack surface — such as exposed VPNs or misconfigured Simple Storage Service (S3) buckets — matches the current threat landscape. Third, AI-generated user and operator activity produces realistic background traffic — like logins, document edits, and OT interactions — that creates a "lived-in" noise floor validating the environment to intruders.[17] Finally, automated deception updates apply fixes based on red-team findings and new threat intelligence, refreshing credentials, system images, and network topologies.

The result is a dynamic deception environment. By automating adaptation, OHMAD compels adversaries to waste time and resources validating targets, knowing that any interaction may expose their tools, infrastructure, and revenue streams.

IV. Governance, Sustainability, and Cost

Actor	**Role in OHMAD**
Oil & Natural Gas Sector Coordinating Council (ONG SCC)	Central coordinator; convenes operators, vendors, researchers, and insurers; aligns with DOE/CISA
Pipeline Operators	Fund honeypots; secure real OT
Pipeline vendors (Honeywell, Microsoft, Siemens)	Provide ICS protocol simulations and vulnerability data
Cybersecurity Firms (Mandiant, CrowdStrike, Dragos)	Build a deception network; conduct red-teaming

[15] Andrew Rogers and Temmie Shade, "Building the Science of Defensive Cyber Deception," *The Next Wave 23* (2021), https://www.govinfo.gov/content/pkg/GPO-TNW-23-1-2021/pdf/GPO-TNW-23-1-2021-3.pdf
[16] Birchwood University, "Is Agentic AI the Future of Cyber Defense?," August 2025, https://www.birchwoodu.org/is-agentic-ai-the-future-of-cyber-defense/
[17] Shaik Abdul Kareem, Ram Chandra Sachan, and Rajesh Kumar Malviya, "AI-Driven Adaptive Honeypots for Dynamic Cyber Threats," *SSRN Working Paper*, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4966935; Luis O. Noguerol, "AI-Generated Honeypots That Learn and Adapt," *Cybersecurity Tribe*, June 26, 2025, https://www.academia.edu/125246186/AI_Driven_Adaptive_Honeypots_for_Dynamic_Cyber_Threats

Cloud Providers (AWS, Azure)	Host scalable honeypot environments
Crypto Analytics Firms (TRM, Chainanalysis)	Monitor and trace wallet addresses in real time
Independent Researchers	Identify new attack paths; improve deception fidelity
Cyber Insurers	Mandate participation as a coverage requirement

OHMAD relies on an industry-led coalition. The Oil & Natural Gas Sector Coordinating Council (ONG SCC) is designated as the central coordinator because it is the formally recognized industry governance body for the oil and natural gas sector within the U.S. critical infrastructure framework. Sector Coordinating Councils are structured to enable industry-led coordination aligned with federal guidance from CISA and the Department of Energy, making the ONG SCC a natural institutional home for OHMAD without expanding federal operational oversight.[18] This approach reflects established public–private governance models for critical infrastructure security.

Non-state leadership enables OHMAD to operate at the speed of ransomware actors. Private-sector entities can rotate credentials, update vulnerabilities, and scale OHMAD without the operational delays that bind federal agencies. At the same time, the government remains a critical partner: the FBI and DOJ act on wallet-tracing intelligence, while CISA provides guidance and alignment with national priorities. This hybrid design preserves industry agility while leveraging the government's investigative and enforcement powers.[19]

OHMAD's annual operating costs, projected to be $50–100 million, pale in comparison to the economic impact of a single ransomware-induced shutdown, which can exceed $1 billion.[20] This estimate is based on cost benchmarks from large-scale, industry-led cybersecurity consortiums and reflects three primary components: (1) cloud infrastructure to operate distributed honeypots and monitoring systems; (2) continuous red-teaming, malware analysis, and credential rotation delivered by private cybersecurity firms; and (3) coordination costs for staffing, legal compliance, and secure intelligence-sharing among pipeline operators, insurers, and federal partners. Funding is structured primarily through private-sector participation, including annual operator fees, in-kind vendor services, and insurer-driven compliance incentives.[21] Beyond direct

[18] U.S. Cybersecurity and Infrastructure Security Agency (CISA), *Energy Sector Oil and Natural Gas Subsector Coordinating Council Charter,* May 2016, https://www.cisa.gov/sites/default/files/publications/energy-ong-scc-charter-2016-508.pdf
[19] U.S. Cybersecurity and Infrastructure Security Agency (CISA), *National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience*, 2013, https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf
[20] David McCann, "Ransomware Attacks Pile Up in Disturbing Trend, New Data Shows," *CFO*, August 9, 2023, https://www.cfo.com/news/-ransomware-attacks-pile-up-in-disturbing-trend-new-data-honeywell-cybersecurity-cfo-/750363/
[21] Shutian Liu and Quanyan Zhu, "Cyber Insurance for Cyber Resilience," *arXiv*, December 5, 2023, https://arxiv.org/html/2312.02921v1

defense, this deception environment imposes operational costs on attackers by diverting time, tools, and attention away from real systems. Over time, AI-driven automation further reduces OHMAD's maintenance burden by continuously updating decoy environments and system configurations.

V. Legal, Regulatory, and Policy Foundations

OHMAD's successful deployment requires compliance with legal and regulatory standards that safeguard private sector actors from civil liability in the process of intelligence collection and information sharing. This necessitates identifying relevant statutory and regulatory safe harbors with the potential to shield actors from liability.

Defensive Operation under the TSA Security Directive

The Transportation Security Administration possesses broad statutory authority under 49 U.S.C. 114 to regulate and ensure security across all transportation modes, including over pipelines. Congress authorizes the TSA to issue directives under 49 U.S.C. §114 sections (f) and (I)(2)(A) to empower its oversight of security responsibilities across modes of transportation. Under 49 U.S.C. §114 (I)(2)(A), the TSA may issue regulations or security directives "immediately in order to protect transportation security", as an emergency procedures regulation.[22]

Following the Colonial Pipeline attack, the TSA exercised this authority by issuing Security Directives (SDs) targeting failures exposed by the attack. These directives focused on incident reporting and the designation of cybersecurity points of contact for the TSA and CISA. [23] They also required operators to conduct vulnerability assessments and develop cybersecurity contingency and recovery plans to minimize operational interruptions.[24] Later iterations of the SDs were performance-based and focused on securing OT systems. They also mandated that operators achieve specific critical security outcomes, such as secure access control measures and annual testing of incident response plans.[25]

Evidently, the TSA is familiar with issuing mandates that are well-tailored to the aim of implementing proactive cyberattack mitigation measures. Obtaining formal TSA and DHS authorization through a mandatory security directive is critical to ensuring OHMAD operations are legally compliant. The TSA's authority, in issuing a security directive, would transform OHMAD from an optional defensive deployment measure into a federally supported, and legally defensible, countermeasure.

---

[22] 49 U.S.C. §114, https://www.law.cornell.edu/uscode/text/49/114
[23] Department of Homeland Security, "Ratification of Security Directives," *Federal Register*, Document No. 2025-01243, January 17, 2025, https://www.federalregister.gov/documents/2025/01/17/2025-01243/ratification-of-security-directives
[24] Shardul Desai and Marissa C. Serafino, "TSA's Pipeline of Cybersecurity Requirements," *Holland & Knight Alert*, August 13, 2021, https://www.hklaw.com/en/insights/publications/2021/08/tsas-pipeline-of-cybersecurity-requirements
[25] Xage, "Complying with TSA Pipeline Security Directives," *Xage*, March 22, 2022, https://xage.com/complying-with-tsa-pipeline-security-directives/#:~:text=TSA%20pipeline%20security%20guidelines%20include,The%20Path%20Forwhigh-valuexceede

With respect to information sharing, the TSA SDs already mandate incident reporting to CISA, so OHMAD would operationalize this by generating high value C2 and financial intelligence, to be reported immediately and legally. Notably, OHMAD's continuous detection and intelligence extraction exceeds TSA's performance-based outcomes for detection and response planning. Mandating OHMAD would be costly, so operators should be rewarded with regulatory compliance credits. The TSA could reward OHMAD deployment through less frequent mandatory audits, and cybersecurity insurers might also be incentivized to offer discounts to operators. This nexus would align private sector financial incentives with national security objections.

Statutory Analog: 47 U.S.C. § 223

47 U.S.C. § 223 offers a statutory analog that may be construed to provide an additional liability shield. This statute contains an immunity principle which provides a safe harbor for common carriers who take good faith actions to restrict access to harmful content (particularly obscenity).[26] OHMAD could be construed as a federally (TSA) authorized defensive operation engaging in a good faith measure to protect critical infrastructure, subject to this immunity principle. This argument relies on analogizing a common carrier to a critical infrastructure operator, who must similarly be shielded from liability when, in good faith, it restricts access to illegal, system-damaging communication such as C2 traffic. However, this is not as strong a legal basis for immunity as an analogy can be attenuated and depends on rules of statutory interpretation, as it's not clear whether this classification can be upheld.

Cryptocurrency Seizure and Reporting

Any ransom payments must be reported pursuant to the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). Through OHMAD, seizures of the adversary's C2 communications within the scheme would provide wallet information before payments are rendered, which allows the DOJ and FBI to accelerate asset tracing and seizure efforts. OHMAD's ability to extract wallet addresses would enable OFAC sanctions, which target specific wallet addresses associated with illicit actors. OHMAD-collected intelligence would provide verified addresses for sanctioning and tracing efforts.

Applicability of Temporary Restraining Orders (TROs)

The use of temporary restraining orders (TROs) in the context of cybersecurity operations can compel the redirection of domain registries and demand service providers to block connection requests from adversaries, such as in GameOverZeus.[27] Its application is less straightforward for OHMAD, as it would be difficult to overcome evidentiary pleading requirements to obtain this order in the absence of specified, imminent, irreparable injury.[28] Should a TRO be obtained and

[26] 47 U.S.C. §223, https://www.law.cornell.edu/uscode/text/47/223
[27] Josephine Wolff, *You'll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches*, Cambridge, MA: The MIT Press, 2018, chap. 4, 67.
[28] Fed. R. Civ. P. 65, https://www.law.cornell.edu/rules/frcp/rule_65

served on a cryptocurrency exchange, it is unlikely that an adversary would comply with such a request. Rather, this legal maneuver is limited in its application here to a potentially narrow set of legitimate third-party service providers who might be able to reveal identified wallet addresses.

VI. Impact, Risk, and Future Evolution

OHMAD aims to reduce the feasibility of ransomware attacks by shifting the initiative back to defenders. From their point of view, OHMAD's impact follows the '3Pre' concept: it 'pre-builds' the deception environment, 'pre-blocks' adversarial tools based on mirror telemetry, and 'pre-seizes' criminal proceeds with help from federal authorities. From the attackers' perspective, OHMAD introduces uncertainty where they normally enjoy confidence. Research shows that decoy assets can deceive attackers when they are not aware.[29] Even with full awareness of decoy assets, exposure to deceptive environments can cause attackers to question the authenticity of their intrusion.[30] In some cases, this uncertainty may prompt attackers to abandon the operation altogether due to concerns about being misled, monitored, or ultimately identified.[31]

How OHMAD Differs from Traditional Honeypots

Similar honeypot systems, like Conpot or Cowrie, have been valuable for academic understanding of attacker behavior but are fundamentally passive, static, and often designed for low-interaction.[32] They do not — because they have not been designed to — replicate pipeline architectures in convincing detail, simulate OT signals that matter to critical infrastructure attackers, and they do not link intelligence to rapid disruption workflows.[33]

OMHAD departs from these models. It uses real compromised credentials where possible, mirrors the legacy systems and weak access paths that attackers actually exploit, and supports high-interaction engagements that keep affiliates inside the mirror long enough to reveal their tooling and infrastructure. Most importantly, OHMAD treats intelligence as a trigger for action: operators share IOCs quickly, infrastructure partners sinkhole C2 nodes, and law enforcement gets wallet data early enough to disrupt payments. As a result, organizations may be able to reduce the cost and impact of incidents more effectively than with prior techniques.

---

[29] Andrew Rogers and Temmie Shade, "Building the Science of Defensive Cyber Deception," *The Next Wave*, vol. 23, 2021, 9, https://www.govinfo.gov/content/pkg/GPO-TNW-23-1-2021/pdf/GPO-TNW-23-1-2021-3.pdf

[30] Rogers and Shade, "Building the Science of Defensive Cyber Deception," 23:9–10.

[31] *Ibid.*, 10.

[32] Youness Ghazi, Mohamed Tabaa, Ghita Zaz, and Mohamed Ennaji, "Ontology-Driven Semantic Honeypot with Digital Twin Integration for Context-Aware Cyber Deception in Industrial OT Systems," in *Proceedings of the 32nd IEEE International Conference on Electronics, Circuits and Systems (ICECS)* (Marrakech, Morocco, November 17–19, 2025) (IEEE, 2025), https://doi.org/10.1109/ICECS66544.2025.11270675; Anastasia Safargalieva and Emmanouil Vasilomanolakis, "Towards Bio-Inspired Cyber-Deception: A Case Study of SSH and Telnet Honeypots," in Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (Venice, Italy, June 30–July 4, 2025) (IEEE, 2025), https://doi.org/10.1109/EuroSPW67616.2025.00079

[33] The lack of realism and dynamism in traditional honeypot models allowed experienced attackers to often identify and avoid them. Moreover, they are poorly suited to detecting or analyzing modern, highly sophisticated attack techniques. See: Shaik Abdul Kareem, Ram Chandra Sachan, and Rajesh Kumar Malviya, "AI-Driven Adaptive Honeypots for Dynamic Cyber Threats," *SSRN Working Paper*, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4966935

Risk Management

OHMAD raises two key concerns. First, attackers, should they recognize the mirror environment as a decoy, may retaliate. This risk is diminished through distribution: attackers cannot easily identify which operator hosts which mirror, and the coalition can raise baseline defenses across participants. Second, adversaries could leverage counter-deception tactics, including AI-enabled decoys designed to mislead defenders. This threat will grow. Defenders should plan for it now rather than treat it as hypothetical. OHMAD's deployment of agentic AI tooling also creates governance and ethics questions. Defenders need clear boundaries for what AI agents can do, how they collect and store data, and how they engage with adversaries.[34] As noted, a TSA-backed framework can help set those guardrails, especially when it comes to questions of "ethical hacking," especially as OHMAD scales across the sector.[35]

Cross-Sector Scalability

Private pipelines offer the primary test case, not the only one. Water systems, electric grids, manufacturing, and healthcare face the same ransomware dynamics: stolen credentials, aging systems, and disruption under extreme time pressure. Attackers reuse the same tools and access brokers across these sectors. Thus, a credential-triggered deception layer provides early warning for critical infrastructure that spans well beyond pipelines. As mentioned, cyber insurers can speed adoption by tying coverage and pricing to participation, moving OHMAD from a best practice to a baseline expectation.

Conclusion

OHMAD reframes how critical private pipeline operators defend themselves against ransomware. It shifts the fight from reacting after compromise to shaping engagement with ransomware groups before any damage occurs. By pulling adversaries into a controlled mirror environment, OHMAD transforms intrusion attempts into intelligence, and in linking that intelligence to coordinated disruption — blocking malware, dismantling infrastructure, supporting attribution, and seizing payments — it raises attacker costs and lowers the odds of success. Ransomware groups will persist, but OHMAD aims to make pipelines across North America impenetrable to attacks in a way that scales: industry-led, government-supported, and built for continuous adaptation. If most "viable access" looks real but leads nowhere, attackers will stop treating critical infrastructure as easy targets. That is the objective, one which OHMAD is more than capable of achieving.

---

[34] Birchwood University, "Is Agentic AI the Future of Cyber Defense?," August 2025, https://www.birchwoodu.org/is-agentic-ai-the-future-of-cyber-defense//; Suchi Rudra, "AI Creates Realistic Honeypots for Cybersecurity," *EdTech Magazine*, December 7, 2025, https://edtechmagazine.com/k12/article/2025/01/ai-powered-honeypots-cybersecurity-perfcon

[35] *Ibid.*

Bibliography

Birchwood University. “Is Agentic AI the Future of Cyber Defense?” August 2025. https://www.birchwoodu.org/is-agentic-ai-the-future-of-cyber-defense/.

“Colonial Pipeline CEO Testifies about Cyberattack at Senate Hearing.” YouTube video. Uploaded June 8, 2021. Accessed December 13, 2025. https://www.youtube.com/watch?v=KVvvGQ3mFjs.

Department of Homeland Security. “Ratification of Security Directives.” *Federal Register*, Document no. 2025-01243, January 17, 2025. https://www.federalregister.gov/documents/2025/01/17/2025-01243/ratification-of-security-directives.

Department of Justice. 2021. "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists DarkSide." Press Release, June 7, 2021. https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

Desai, Shardul, and Marissa C. Serafino. “TSA’s Pipeline of Cybersecurity Requirements.” *Holland & Knight Alert*, August 13, 2021. https://www.hklaw.com/en/insights/publications/2021/08/tsas-pipeline-of-cybersecurity-requirements.

De Vynck, Gerrit, Rachel Lerman, Ellen Nakashima, and Chris Alcantara. “The Anatomy of a Ransomware Attack.” *The Washington Post*, July 9, 2021. https://www.washingtonpost.com/technology/2021/07/09/how-ransomware-attack-works/.

Fed. R. Civ. P. 65. https://www.law.cornell.edu/rules/frcp/rule_65.

Fung, Brian, and Geneva Sands. “Colonial Pipeline CEO Tells Congress Company Did Not Have Backup Plan Before Ransomware Attack.” *CNN*, June 8, 2021. https://www.cnn.com/2021/06/08/politics/colonial-pipeline-ceo-on-capitol-hill-ransomware.

Ghazi, Youness, Mohamed Tabaa, Ghita Zaz, and Mohamed Ennaji. “Ontology-Driven Semantic Honeypot with Digital Twin Integration for Context-Aware Cyber Deception in Industrial OT Systems.” In *Proceedings of the 32nd IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, Marrakech, Morocco, November 17–19, 2025. IEEE, 2025. https://doi.org/10.1109/ICECS66544.2025.11270675.

Javadpour, Amir, Forough Jaʿfari, Tarik Taleb, Mohammad Shojafar, and Chafika Benzaïd. “A Comprehensive Survey on Cyber Deception Techniques to Improve Honeypot Performance.” *Computers & Security* 140 (2024): 103792. https://doi.org/10.1016/j.cose.2024.103792.

Kareem, Shaik Abdul, Ram Chandra Sachan, and Rajesh Kumar Malviya. “AI-Driven Adaptive Honeypots for Dynamic Cyber Threats.” *SSRN Working Paper*, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4966935.

McCann, David. “Ransomware Attacks Pile Up in Disturbing Trend, New Data Shows.” *CFO*, August 9, 2023. https://www.cfo.com/news/-ransomware-attacks-pile-up-in-disturbing-trend-new-data-honeywell-cybersecurity-cfo-/750363/.

Microsoft. *Microsoft Digital Defense Report 2025*. 2025. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf.

Noguerol, Luis O. “AI-Generated Honeypots that Learn and Adapt.” *Cybersecurity Tribe* (blog), June 26, 2025. https://www.cybersecuritytribe.com/articles/ai-generated-honeypots-that-learn-and-adapt#:~:text=distinguish%20between%20genuine%20threats%20and%20benign%20activity.

Palo Alto Networks Unit 42. “Extortion and Ransomware Trends, January–March 2025.” *Unit 42*, April 23, 2025. https://unit42.paloaltonetworks.com/2025-ransomware-extortion-trends/.

Pekoske, David P. “Pipeline Cybersecurity: Protecting Critical Infrastructure.” Testimony before the Senate Committee on Commerce, Science, and Transportation, *Transportation Security Administration*, July 27, 2021. https://www.tsa.gov/news/press/testimony/2021/07/27/pipeline-cybersecurity-protecting-critical-infrastructure.

Reuters. 2021. "U.S. Seizes $2.3 Mln in Bitcoin Paid to Colonial Pipeline Hackers." *Reuters*, June 7, 2021. https://www.reuters.com/business/energy/us-announce-recovery-millions-colonial-pipeline-ransomware-attack-2021-06-07/.

Rogers, Andrew, and Temmie Shade. “Building the Science of Defensive Cyber Deception.” *The Next Wave*. Vol. 23, 2021. https://www.govinfo.gov/content/pkg/GPO-TNW-23-1-2021/pdf/GPO-TNW-23-1-2021-3.pdf.

Rudra, Suchi. “AI Creates Realistic Honeypots for Cybersecurity.” *EdTech Magazine*, December 7, 2025. https://edtechmagazine.com/k12/article/2025/01/ai-powered-honeypots-cybersecurity-perfcon#:~:text=more%20realistic%20and%20highly%20convincing%20honeypots.

Sanger, David E., and Nicole Perlroth. “White House Warns Companies to Act Now on Ransomware Defenses.” *The New York Times*, June 3, 2021. https://www.nytimes.com/2021/06/03/us/politics/ransomware-cybersecurity-infrastructure.html.

Safargalieva, Anastasia, and Emmanouil Vasilomanolakis. “Towards Bio-Inspired Cyber-Deception: A Case Study of SSH and Telnet Honeypots.” In *Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Venice, Italy, June 30–July 4, 2025. IEEE, 2025. https://doi.org/10.1109/EuroSPW67616.2025.00079.

Liu, Shutian, and Zhu, Quanyan. “Cyber Insurance for Cyber Resilience.” *arXiv,* December 5, 2023. https://arxiv.org/html/2312.02921v1

Tarabay, Jamie. “Trump Administration Turning to Private Firms in Cyber Offensive.” *Yahoo Finance*, December 12, 2025. https://finance.yahoo.com/news/trump-administration-turning-private-firms-191259484.html.

U.S. Cybersecurity and Infrastructure Security Agency (CISA). “Advisory AA21-076A: TrickBot Malware.” March 17, 2021. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-076a.

U.S. Cybersecurity and Infrastructure Security Agency (CISA). *Energy Sector Oil and Natural Gas Subsector Coordinating Council Charter*. May 2016. https://www.cisa.gov/sites/default/files/publications/energy-ong-scc-charter-2016-508.pdf.

U.S. Cybersecurity and Infrastructure Security Agency (CISA). *National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience*. 2013. https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf.

U.S. Department of Justice. “Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists DarkSide.” Press release, June 7, 2021. https://www.justice.gov/archives/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

Vorndran, Bryan A. “Ransomware: Attacks and Defenses.” Statement before the Senate Committee on the Judiciary, Washington, DC, July 26, 2021. https://www.judiciary.senate.gov/download/bryan-vorndran-727-testimony?download=1.

Vorndran, Bryan A. “Oversight of the Federal Bureau of Investigation, Cyber Division.” Statement before the House Committee on the Judiciary, Washington, DC, March 29, 2022. https://docs.house.gov/meetings/JU/JU00/20220329/114533/HHRG-117-JU00-Wstate-VorndranB-20220329.pdf

Walden, Todd, and Steve Hill. “A Simple Solution for More Secure Pipelines.” *Emerson Automation Experts*, January 3, 2023. https://www.emersonautomationexperts.com/2023/control-safety-systems/a-simple-solution-for-more-secure-pipelines/.

What Is DarkSide Ransomware? Akamai Glossary. December 13, 2025. https://www.akamai.com/glossary/what-is-darkside-ransomware.

Wolff, Josephine. *You'll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches*. Cambridge, MA: MIT Press, 2018.

Xage. "Complying with TSA Pipeline Security Directives." *Xage*, March 22, 2022. https://xage.com/complying-with-tsa-pipeline-security-directives/.

49 U.S.C. § 114. https://www.law.cornell.edu/uscode/text/49/114.

47 U.S.C. § 223. https://www.law.cornell.edu/uscode/text/47/223.

AI-Use Disclosure

Our team used ChatGPT during the process of developing this paper for three distinct purposes:

1) Given the post-presentation feedback we received from Professor Healey regarding the inadequacy of the original acronym for this system, we used the LLM to brainstorm new titles for the project, and ultimately decided to opt for the first suggestion offered: "The Operational Honeypot Mirror for Adversary Disruption".

2) We then used the LLM to generate a rough outline of the paper, using text from the team's original slides in our prompt and feedback received from Professors Healey and Carmakal over email, as well as feedback recorded following the in-class presentation of this idea.

> **Prompt:** Generate a paper outline for this presentation that attends to feedback (inserting professors' comments).
>
> **Response:**
>
> **<u>O.H.M.A.D.: Concept and Rationale</u>**
>
> **What it is:** O.H.M.A.D. is a sector-led deception system that uses high-fidelity IT/OT mirrors to lure ransomware affiliates into controlled environments, capture their activity, and trigger coordinated disruption.
>
> **What makes it different:** Unlike traditional honeypots, O.H.M.A.D. is operational, sector-specific, and designed for early warning and real-world disruption—not research observation.
>
> **<u>How O.H.M.A.D. Works: Technical and Operational Design</u>**
>
> **Phase 1: Building the Deception Environment**
> - Mirror real pipeline IT and OT architectures.
> - Replicate known weaknesses (e.g., legacy VPNs without MFA).
> - Populate realistic data (billing systems, internal documents, pipeline maps).
> - Seed real compromised credentials to attract active affiliates.
>
> **Phase 2: Instrumented Observation**
> - Monitor all mirror activity with EDR and network telemetry.

- Treat all activity as malicious by definition.
- Extract malware samples, C2 infrastructure, tactics, and ransom wallets in real time.

Phase 3: Multi-Pillar Disruption (Vorndran Framework)

- Malware: Rapid IOC sharing through ISACs and security vendors.
- Infrastructure: Sinkhole or disable C2 servers via cloud and ISP partners.
- Communication: Share behavioral patterns with FBI/CISA for attribution.
- Payment: Identify wallets early and support DOJ seizure actions.

Phase 4: Continuous Evolution

- **Update vulnerabilities and artifacts regularly.**
- **Use AI-driven red teams to test and refresh realism.**
- **Share improvements across all participating operators.**

Governance and Sustainability

Who runs it: An industry-led coalition coordinated through the Oil & Natural Gas Sector Coordinating Council.

Who participates: Pipeline operators, OT vendors, cybersecurity firms, cloud providers, crypto analytics companies, insurers, and independent researchers.

Government role: Supportive but not operational—law enforcement handles seizures and attribution; regulators provide alignment and safe harbors.

Why it lasts: Annual costs are modest compared to outage losses, and insurers can drive adoption by tying participation to coverage.

Legal and Policy Framework

TSA security directives provide the strongest legal foundation for authorizing deception-based defense.

ISAC-based sharing mitigates antitrust risk.

CIRCIA reporting aligns with early wallet and C2 intelligence.

DOJ/FBI coordination enables lawful tracing, sanctions, and seizure of ransom proceeds.

Why O.H.M.A.D. Beats the Status Quo

Moves detection from post-breach to pre-impact.

Raises attacker costs across the entire ransomware business model.

Turns intrusions into intelligence instead of incidents. Makes pipelines unattractive targets rather than soft ones.

Risks and Mitigations

Retaliation: Distributed design obscures attribution and raises collective defense.

Deception discovery: Rotating vulnerabilities and AI-driven variation preserve realism.

Noise: Isolated mirrors eliminate false positives.

Implementation Path

Pilot: Deploy with a small group of major pipeline operators.

Scale: Expand to 50+ operators and formalize ISAC workflows.

Institutionalize: Embed AI evolution, insurance incentives, and regulatory recognition.

Conclusion

O.H.M.A.D. offers a practical, scalable way to disrupt ransomware before it reaches real systems. It shifts critical infrastructure defense from reaction to initiative by changing where and how attackers engage.

3) Finally, after collectively modifying the outline, determining additional elements that the paper would require, and drafting each section, the LLM (in addition to Grammerly) was used to scan for grammatical errors, which were subsequently revised when spotted.