SITJOURNAL
Security Intelligence Terrorism Journal

Security Intelligence Terrorism Journal (SITJ), Vol. 03 No. 01 (2026), pp. 16-21
Research Article
doi: https://doi.org/10.70710/sitj.v3i1.82

Strategic Blindness in Outer Space: Asymmetric Threat Analysis of Starlink on Indonesia's Cyber Sovereignty and Intelligence Mitigation Strategies

Ahmad Ridwansyah[1,a,*], Pratama Dahlian Persadha[1,b], Edy Supriadi[1,c]

[1]Sekolah Tinggi Intelijen Negara, Bogor, Indonesia
[a]ridwan@ombudsman.go.id; [b]pratama@cissrec.org; [c]edyyadi2@gamil.com
*Corresponding author

Article Info
Received: 28-Dec-2025
Revised: 6-Jan-2026
Accepted: 6-Jan-2026

Keywords
Asymmetric Threat; Cyber Sovereignty; Intelligence Strategy; Starlink; National Security

Abstract
The advent of Low Earth Orbit (LEO) satellite constellations, epitomized by SpaceX's Starlink, has fundamentally disrupted the global telecommunications architecture. While offering critical connectivity solutions for archipelagic nations like Indonesia, this technology simultaneously introduces profound asymmetric threats to national security. This study aims to analyze the anatomy of these threats, evaluate their multidimensional impacts, and formulate a comprehensive intelligence strategy to mitigate the hegemony of Starlink's technology. Adopting a post-positivist paradigm, this research utilizes a qualitative descriptive method integrated with the Intelligence Analysis Cycle. The findings indicate that the threat level of Starlink is 'Critical' based on Hank Prunckun's threat matrix (T = I x C), driven predominantly by uncontrolled technical capabilities rather than malicious intent. Starlink is identified as bypassing national gateways, creating "strategic blindness" for intelligence apparatuses, and acting as a force multiplier for separatist groups via anti-jamming communication capabilities. Economically, its dominance threatens to de-industrialize local telecommunications infrastructure through predatory pricing. The study recommends a mitigation strategy based on Arthur F. Lykke Jr.'s model, advocating for "Market Power Diplomacy," the establishment of independent Space Situational Awareness (SSA), and the implementation of a hardware ban as an ultimum remedium.

1. Introduction

The trajectory of global communication technology over the past two decades has marked a fundamental shift in the control of data spaces, where non-state actors now possess infrastructure capabilities that rival or even surpass those of sovereign states. This phenomenon is most visibly manifested through the proliferation of Starlink, a Low Earth Orbit (LEO) satellite constellation operated by SpaceX, which offers low-latency, high-speed global internet access (Molla, 2024). For Indonesia, the world's largest archipelagic state with numerous "blank spot" areas, this technology presents a compelling solution for digital equity. However, from a national security perspective, Starlink's direct-to-user architecture creates severe strategic vulnerabilities.

The entry of Starlink without the mandatory routing through a national Network Operation Center (NOC) and Internet Gateway implies a significant erosion of the state's capacity as an informational "Gatekeeper." This condition stands in direct contradiction to the principle of Digital Sovereignty, which necessitates full state control over data flows within its jurisdiction (Pohle & Thiel, 2020). The ability of LEO satellites to beam internet directly to user terminals bypasses traditional chokepoints—such as

submarine cable landing stations and terrestrial backbones—rendering conventional censorship and surveillance mechanisms obsolete.

Current studies often overlook how dual-use commercial technologies can be weaponized by non-state actors in conflict zones or how they create intelligence gaps for state security apparatuses. This research aims to bridge this gap by employing an intelligence analysis approach to dissect the threat anatomy, evaluate its multidimensional impacts, and formulate an effective mitigation strategy.

2. Literature Review

2.1. Threat Analysis Theory

To measure the level of danger posed by non-traditional actors, this study employs Hank Prunckun's (2019) Threat Analysis Theory. Prunckun posits that a Threat (T) is the product of an actor's Intent (I) and Capability (C), expressed as T = I x C. Intent is further decomposed into Desire (D) and Expectation (E), while Capability comprises Knowledge (K) and Resources (R). In the context of Starlink, this framework allows for a nuanced assessment where capability (technological dominance) may outweigh intent (commercial motivation) in constituting a national security threat.

2.2. National Security and Strategic Intelligence

The concept of national security is analyzed using Paul D. Williams' (2008) multidimensional framework, which extends security beyond military defense to include economic, political, and societal dimensions. This is critical for understanding how Starlink impacts not just border security but also economic resilience and cyber sovereignty. Furthermore, the formulation of state response is guided by Arthur F. Lykke Jr.'s (1997) Strategic Model, which balances Ends (objectives), Ways (concepts), and Means (resources) to ensure a coherent and sustainable mitigation strategy.

3. Method

This study adopts a qualitative descriptive design rooted in a post-positivist paradigm, allowing for theexploration of complex, dynamic security phenomena through deep interpretation of empirical data. The research locus focuses on the intersection of technology policy and national defense in Indonesia. Data collection was conducted through semi-structured interviews with five purposively selected key informants (subject matter experts) from strategic institutions:

1. State Intelligence Agency (BIN) – focusing on threat detection.
2. National Cyber and Crypto Agency (BSSN) – focusing on cyber defense.
3. National Research and Innovation Agency (BRIN) – focusing on space technology.
4. Coordinating Ministry for Political, Legal, and Security Affairs – focusing on policy harmonization.

The data analysis technique integrates NVivo 12 Pro software for rigorous thematic coding and the Intelligence Analysis Cycle (Sugirman, 2009), which comprises four stages: Judgment, Early Warning, Forecasting, and Problem Solving. Data validity was established through source triangulation across agencies to minimize researcher subjectivity and ensure a comprehensive perspective.

4. Results

4.1. The Anatomy of the Starlink Threat: Dominance of Capability

Referring to Hank Prunckun's threat matrix, this research finds that the Starlink threat level is Critical/High, driven overwhelmingly by the Capability variable (C), despite the service provider's Intent (I) being ostensibly commercial. The analysis reveals that Starlink's Capability—comprising thousands of satellites, advanced end-to-end encryption, and beam-hopping technology—creates an asymmetric disparity against Indonesia's cyber defense capabilities.

Informants confirmed that the equipment currently available to Indonesia's security apparatus is incapable of intercepting Starlink signals. The presence of Starlink allows all traditional security layers—Seaport, Backbone, Point of Presence—to be bypassed, leaving the user dependent solely on the security protocols of a foreign provider. The absence of physical infrastructure (NOC) within Indonesian territory causes an "Intelligence Blind Spot," rendering conventional Lawful Interception methods ineffective. This technical inability is exacerbated by a Regulatory Gap, where existing regulations are still oriented towards geostationary (GSO) satellites and fail to accommodate the rapid orbital dynamics of LEO constellations.

4.2. Multidimensional Impacts on National Security

Based on Paul D. Williams' framework, the impact of Starlink is not singular but multidimensional, affecting military, economic, and political stability.

4.2.1. Erosion of Cyber Sovereignty

The research findings confirm the failure of the national firewall system. Illegal content, such as online gambling and radical propaganda, which has been successfully blocked on terrestrial ISPs, remains accessible through the Starlink network. This signifies the delegitimization of state authority in enforcing laws within the cyber domain. The state effectively loses its digital borders, creating a "tunnel" for illicit information flow that is immune to national jurisdiction.

4.2.2. Asymmetric Military Threat (The Force Multiplier Effect)

In the military domain, Starlink acts as a force multiplier for non-state actors, particularly separatist groups and terrorist organizations operating in the 3T (frontier) regions. Starlink's ability to provide global connectivity that is resistant to jamming allows terrorist groups to coordinate attacks, manage logistics, and facilitate digital financing from blank spot areas that were previously isolated. Furthermore, the study identified an evolution in counter-intelligence tactics, such as the use of third-party proxies for device procurement to obscure ownership and intermittent transmission patterns to evade signal detection.

4.2.3. Economic Threat to Critical Infrastructure

The dominance of Starlink's economic of scale creates a high risk of predatory pricing, which threatens the viability of local telecommunications operators (SOEs and private sector). If local operators collapse, Indonesia faces the prospect of absolute dependence on foreign infrastructure. This constitutes a strategic vulnerability in National Resilience, as the state would lack independent communication backbones during geopolitical crises or trade wars.

4.3. Intelligence Strategy Formulation: Ends, Ways, and Means

To mitigate these threats, the research formulates an intelligence strategy based on Arthur F. Lykke Jr.'s model:

- Ends (Strategic Objectives): The primary objective is to uphold Data Sovereignty and ensure Economic Resilience without impeding technological access for citizens in remote areas.
- Ways (Operational Concepts): Operational strategies must shift from purely technical approaches to hybrid methodologies:
    - Market Power Diplomacy: Leveraging Indonesia's market access of 270 million people as a bargaining chip to coerce Starlink into complying with national governance standards, such as establishing a local NOC.
    - Financial Intelligence (FININT): Shifting detection focus from physical signal interception (which is technically difficult) to tracking banking payment trails to identify illegal users.
    - Ultimum Remedium: The implementation of a hardware ban and the interdiction of physical distribution chains if regulatory compliance is not achieved.
- Means (Resources): The state must invest in independent monitoring capabilities. Indonesia urgently requires the acquisition of independent Space Situational Awareness (SSA) capabilities,

specifically optical sensors and radar, and the establishment of a cross-sectoral 'NGSO Office' to verify spectrum data independently.

5. Conclusion

The threat posed by Starlink to Indonesia's national security is not merely technical but systemic and asymmetric, fundamentally challenging the state's Westphalian sovereignty in the digital age. This technology acts as a double-edged sword; while promising digital inclusion, it paralyzes cyber sovereignty through its direct-to-consumer gateway bypass mechanism. This architectural circumvention renders national firewalls and lawful interception protocols obsolete, effectively creating a "sovereign-free" digital tunnel within Indonesian territory. Furthermore, Starlink serves as a potent force multiplier for non-state actors, particularly in conflict-prone regions. By providing low-latency, anti-jamming, and encrypted communications to separatist groups, it shifts the tactical balance in asymmetric warfare, complicating counter-insurgency operations and intelligence gathering.

Economically, the unchecked dominance of such mega-constellations threatens the sustainability of national critical information infrastructure (CII). The potential for predatory pricing driven by global economies of scale poses a de-industrialization risk to local telecommunications operators, fostering a dangerous strategic dependence on foreign entities for vital connectivity. Consequently, conventional defense strategies, which rely heavily on terrestrial choke points and territorial jurisdiction, are no longer adequate to address these transnational, orbital threats.

To regain strategic agency, Indonesia must immediately pivot towards a robust, layered defense strategy comprising three core pillars. First, the implementation of coercive regulations is paramount. This entails mandating the construction of local Network Operation Centers (NOCs) and physical gateways as non-negotiable conditions for licensing, ensuring that all data traffic is subject to national lawful interception standards. Second, the state must prioritize the strengthening of independent surveillance infrastructure, specifically Space Situational Awareness (SSA). Without independent radar and optical sensors to verify spectrum usage and orbital maneuvers, Indonesia remains in a state of "strategic blindness," reliant on third-party data. Third, the government must leverage Market Power Diplomacy. With a digital market of over 270 million users, Indonesia possesses significant bargaining leverage to compel compliance from global technology giants, trading market access for adherence to digital sovereignty norms.

Ultimately, this struggle for control over the information space requires decisive political leadership. Should persuasive diplomatic and regulatory measures fail to secure compliance, the state must possess the political will to enforce ultimum remedium measures. This includes the strict prohibition of hardware circulation, the interdiction of illicit supply chains, and the revocation of operational licenses. Preserving the integrity of national sovereignty is not an option but a mandate; allowing a commercial entity to operate above the law sets a perilous precedent that could undermine the very foundation of the nation- state in the 21st century.

References

Betz, D. (2015). *Cyberpower and National Security*. Edinburgh University Press.

Boley, A., Wright, E., Lawler, S., Hickson, P., & Balam, D. (2021). Plaskett 1.8 m Observations of Starlink Satellites. *The Astronomical Journal*, *163*. https://doi.org/10.3847/1538-3881/ac5599

Cavelty, M. D. (2009). *Cyber-security and resilience: a framework for the analysis of critical information infrastructure protection. International Journal of Critical Infrastructure Protection*, 2(3), 146-153.

Chaudhry, A., & Yanikomeroglu, H. (2021). Laser Intersatellite Links in a Starlink Constellation: A Classification and Analysis. *IEEE Vehicular Technology Magazine*, *16*, 48–56. https://doi.org/10.1109/MVT.2021.3063706

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

_____, & Poth, C. N. (2016). *Qualitative inquiry & research design* (4th ed.). SAGE Publications.

CSIS (Center for Strategic & International Studies). (2020). *Defending the Digital Frontier: Critical Infrastructure and National Security in the Information Age*. CSIS.

Duan, T., & Dinavahi, V. (2021). Starlink Space Network-Enhanced Cyber–Physical Power System. *IEEE Transactions on Smart Grid*, *12*, 3673–3675. https://doi.org/10.1109/TSG.2021.3068046

Gunawan, B., & Ratmono, B. M. (2022). *Kuasa Siber: Sebuah Refleksi Kritis*. PT. Rayyana Komunikasindo.

Halferty, G., Reddy, V., Campbell, T., Battle, A., & Furfaro, R. (2022). Photometric characterization and trajectory accuracy of Starlink satellites: implications for ground-based astronomical surveys. *Monthly Notices of the Royal Astronomical Society*. https://doi.org/10.1093/mnras/stac2080

Harianja, A., Rio, A., & Setiawan, M. (2022). IMPLIKASI PERANG SIBER ANTARA ISRAEL, AMERIKA SERIKAT DAN IRAN MELALUI OLIMPIC GAME OPERATION TERHADAP FASILITAS PROGRAM NUKLIR IRAN PADA PERIODE PEMERINTAHAN MAHMOUD AHMADINEJAD: PERANG SIBER STUXNET 2010. *Jurnal Hubungan Internasional Moestopo*. https://journal1.moestopo.ac.id/index.php/mjir/article/download/1895/1094

Harrison, T., & Johnson, K. (2023). *Space Threat Assessment 2023*. *Center for Strategic & International Studies (CSIS).* 180

Intelligence and National Security Alliance (INSA). (2021). *Insider Threats and Commercial Espionage: Economic and National Security Impacts*. INSA.

Iskandar, M. (2025). Serangan Siber: Jenis, Dampak, dan Cara Mengatasinya. In *Phintraco*. https://phintraco.com/serangan-siber/

Karas, J., & Molla, A. M. (2023). *Starlink and the Geopolitics of Space: How Low Earth Orbit Satellite Constellations are Changing the Global Order*. *Chatham House.*

Kelly, T. (2012). *International Internet Bandwith: Supply and Demand*. ITU Workshop.

Kemp, S. (2024). *Digital 2024: Global Overview Report*. DataReportal in partnership with We Are Social and Meltwater. https://datareportal.com/reports/digital-2024-global-overview-report

Kent, S. (1949). *Strategic Intelligence for American World Policy*. In Princeton University Press.

Khoirunnisa. (2024). Cyber Warfare Strategies in the Russia-Ukraine Conflict 2021-2022. *Journal of Information Systems and Technology Management*. https://www.researchgate.net/publication/384774336_Cyber_Warfare_Strategies_in_the_Russia-Ukraine_Conflict_2021-2022

Kraiwanit, T., Limna, P., & Siripipatthanakul, S. 2023. NVivo for Social Sciences and Management Studies: A Systematic Review. Advance Knowledge for Executives, 2(3).

Leiner, B. (1997). *Brief History of The Internet*. Internet Society.

Levchenko, I., Xu, S., Wu, Y.-L., & Bazaka, K. (2020). Hopes and concerns for astronomy of satellite constellations. *Nature Astronomy*, 1–3. https://doi.org/10.1038/s41550-020-1141-0

Lykke, A. F. (1997). Defining military strategy. Military Review, 77(1), 183–186.

Michel, F., Trevisan, M., Giordano, D., & Bonaventure, O. (2022). A first look at starlink performance. *Proceedings of the 22nd ACM Internet Measurement Conference*. https://doi.org/10.1145/3517745.3561416

Milevski, L. (2011). Stuxnet and Strategy. *Joint Force Quarterly*, *63*, 64–69. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-63/jfq-63_64-69_Milevski.pdf?ver=Jy0SW9E8UBbatlrmrw-egQ%3D%3D

Molla, A. M. (2024). *Geopolitics of Starlink: The race for low-Earth orbit satellite dominance. Space Policy*, 67, 101633.

Pohle, J., & Thiel, T. (2020). *Digital sovereignty. Internet Policy Review*, 9(4).

Prunckun, H. (2019). *METHODS OF INQUIRY FOR INTELLIGENCE ANALYSIS (3rd ed.)*. The Rowman & Littlefield Publishing Group, Inc. 181

Rahimi, & Jones. (2025). Cyber warfare dalam Konflik Modern: Analisis Serangan Stuxnet pada Fasilitas Nuklir Iran. *DIALOGIKA*, *1*(3), 49–50. https://ejournal.appisi.or.id/index.php/Dialogika/article/download/372/323

Stuxnet: Titik Balik dalam Konflik Modern. (2025). *DIALOGIKA*. https://ejournal.appisi.or.id/index.php/Dialogika/article/download/372/323/1883

Sugiyono. (2013). *Metode Penelitian Kuantitatif Kualitatif dan R&D* (19th ed.). Alfabeta.

Sukarno, I. (2014). *Ilmu Intelijen*. Prenadamedia Group.

Sugirman, S. (2009). Manajemen Intelijen: Teori dan Aplikasi. Jakarta: PT RajaGrafindo Persada.

Utama, A. (2024, October 8). *Wawancara eksklusif Egianus Kogoya – Perselisihan internal OPM, tuduhan terima suap, dan ancaman 'akan terus bikin pusing Indonesia'*. Https://Www.Bbc.Com/Indonesia/Articles/Cly3z71x4vdo.

Vlaj, S. (2017). *The Role of Non-State Actors in Cyber Security Governance. Lex Localis - Journal of Local Self-Government*, 15(4), 729-747.

Waruwu, B. (2023). *Metode penelitian sosial: Teori dan praktik*. Deepublish.

Wikipedia contributors. (2025, June 1). *Bell Labs*. Https://En.Wikipedia.Org/w/Index.Php?Title=Bell_Labs&oldid=1293333710.

Williams P. (2008). *Security Studies: An Introduction*. Routledge.

Yin, R. K. (2016). Family and Consumer Sciences Research Journal. *Qualitative Research from Start to Finish*, *44*(3).

Yusuf, A. M. (2014). *Metode penelitian: Kuantitatif, kualitatif & penelitian gabungan*. Prenada Media Group.