Starlink in the context of critical infrastructure protection and strategic consequences in cyber warfare: A case study of the Ukraine-Russia conflict and potential utilization by the Papuan separatist groups

Fahmi Ramadan[1*], Fajar Wijitrisnanto[1], Wanodya Esthithama[1], Arip Nurahman[2], Nizar Alam Hamdani[3]

[1]National Cyber and Crypto Agency, Jakarta, Indonesia
[2]Departement of Physics Education, Indonesian Education Institute, Garut, Indonesia
[3]Indonesian Education Institute & Garut University, Garut, Indonesia

Article history
Received: 17 April 2025
Revised: 24 April 2025
Accepted: 26 April 2025

Keywords
Starlink
Cyber warfare
KKB
Critical infrastructure protection

Abstract
The utilization of satellite technology such as Starlink in the context of armed conflict and cyber warfare poses new challenges related to critical infrastructure protection and cyber-crime response strategies. This research explores the role of Starlink technology in the context of critical infrastructure protection and its impact on strategy in cyber warfare, with a focus on a case study of the Ukraine-Russia conflict and its potential utilization by the Papuan Armed Criminal Group (KKB). Using Qualitative Research Thematic Synthesis Method, this research analyzes how Starlink was used during the Ukraine-Russia conflict to maintain communications stability, support military coordination, and maintain internet access for civilians amid disruptions to conventional infrastructure due to Russian attacks. The technology proved to be a crucial element in maintaining reliable communications in the conflict area. In addition, this research highlights the possible use of Starlink by the KKB in Papua to strengthen operational coordination, spread propaganda, and enhance intelligence capabilities. Access to high-speed and secure internet via Starlink could provide a strategic advantage to the KKB, making them more difficult for the Indonesian government to track and intervene. The research also identified strategies that the government and security agencies need to develop to manage and oversee the use of Starlink, such as developing a clear regulatory framework and setting up a cybersecurity coordination center, collaboration with service providers, and the implementation of strong encryption technologies. The results of this study show that while Starlink offers significant benefits in maintaining communications in conflict and remote areas, its uncontrolled use by separatist groups could threaten national stability, requiring a comprehensive strategy to ensure this technology is utilized safely and effectively.

1. Introduction

The development of communication technology has grown rapidly from cable-based communication to satellite-based (Setiawan, 2017). Users also vary from various classes of society from proletariat to elite class. One of the latest innovations that has caught the world's attention is Starlink. Starlink is a satellite network project developed by SpaceX aims to deliver high-speed Internet access around the world (Shaengchart & Kraiwanit, 2024). This technology's benefit is its capacity to offer dependable connectivity in remote regions that are challenging to access with traditional infrastructure. This is an opportunity for Indonesia, which is a country with a large number of islands. The distribution of the islands has an impact on the inequality of the internet contribution rate. Java has the highest contribution of 57.82% while Papua has only 3.79% (Santika, 2024). However, the project not only has an impact on improving internet access in remote areas, but also has strategic implications in the context of critical infrastructure protection and cyber warfare.

*Corresponding author, email: fahmi.ramadan@bssn.go.id

Starlink has come under the spotlight in various international conflicts, one of which is the conflict between Ukraine and Russia. On February 24, 2022, Russia conducted a cyberattack on the KA-SAT GEO ViaSat satellite network used by the Ukrainian army, providing a clear example of the complementary use of cyber operations with conventional military operations on land, sea and air (Urbanus Panggabean et al., 2023). In this conflict, Starlink not only provided internet connectivity for civilians amidst the destruction of telecommunications infrastructure, but also played a role in supporting military operations and strategic communications. The existence of this satellite system adds a new dimension to modern warfare, where information control and security are critical success factors (European Space Policy Institute, 2022). This has not only had a major impact on global politics and the world economy but has also brought renewed focus on the critical role of space in supporting modern militaries, societies and critical infrastructure (Dziwisz & Sajduk, 2023). The battlefield in Ukraine has also been a place of rapid innovation, experimentation, and adaptation, including the combination of SATCOM (Satellite Communication), EO (Earth observation), and PNT (positioning, navigation, and timing) with AI, drones, and other technologies to drive new approaches to C5ISTAR (Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance) (Ogden et al., 2024).

Furthermore, this technology also has the potential to be utilized in various other conflicts, including by armed groups such as the Armed Criminal Group (KKB) in Papua. The KKB conflict in Papua is a very complex issue, involving various interests from local, national, and international actors (Amanda & Pramono, 2023). On the one hand, the KKB is fighting for greater independence and autonomy, often with the support of some indigenous groups and human rights activists. On the other hand, the Indonesian government seeks to maintain its territorial integrity and develop Papua through various development programs (Ismail, 2015). In addition, there are also economic interests from companies operating in the region, especially in the mining sector (Rosyid, 2020). In this complicated situation, the presence of Starlink technology can bring significant changes to conflict dynamics.

Starlink can be utilized by separatist groups such as KKB and their supporters for their communications that cannot be detected by the Indonesian government (Kraz, 2024). This technology has the potential to threaten the integrity of the Republic of Indonesia, as the government will find it difficult to control its use. With easier access to advanced communication technology, these groups can improve their coordination and operational effectiveness, which in turn poses new challenges to law enforcement and national security efforts.

This article aims to examine the role of Starlink in the context of critical infrastructure protection and its strategic consequences in cyber warfare, with a case study of the Ukraine-Russia conflict and its potential utilization by the Papua KKB. Through this analysis, it is hoped to provide a deeper understanding of how modern communication technologies can influence conflict dynamics and defense strategies, as well as the implications for future national security policy.

2. Related Works

The Russia-Ukraine cyber war has been a major focus of research lately. A study published in 2022 by Dr. Herbert Lin delve into the significance of Russian offensive cyber operations against Ukraine (Lin, 2022). These analyses reveal that while Russia did increase cyberattacks before the invasion, their impact wasn't significantly greater than past attempts. Additionally, the attacks focused on disrupting Ukrainian critical infrastructure rather than high-value military targets. The true effectiveness of these tactics in achieving Russian strategic objectives remains unclear due to the ongoing nature of the war.

Marcus Willet in the other opportunity tried to study the nature of cyber warfare between Russia and Ukraine. Through his work, he provides a valuable insight into what the cyber dimension of a modern war might look like (Willett, 2022). His work highlights the resilience of Ukraine's cyber defenses against Russia. Despite facing significant cyber threats from Russia, Ukraine demonstrated remarkable resilience due to its enhanced cybersecurity measures and substantial support from Western allies. This encompassed technical support, intelligence sharing, and the deployment of cybersecurity experts, which collectively helped lessen the impact of Russian cyber-attacks on critical infrastructure and communication networks. The study also delves into the surprising lack of large-scale offensive cyber actions by Russia, potentially due to a focus on intelligence gathering and underestimation of Ukrainian cyber defenses.

Itzhak Aviv on another work explore the broader impact of the conflict on the digital ecosystem (Aviv & Ferri, 2023). The article underscores the critical vulnerabilities exposed in communication

infrastructure during the Russian-Ukrainian conflict, highlighting the necessity for robust backup solutions and the role of commercial satellites like SpaceX's Starlink in maintaining connectivity amidst military tensions. Ukraine's rapid shift to global cloud platforms for sensitive data storage ensured continuity of government services despite physical and cyber threats, emphasizing resilience in crisis management and the evolving significance of communications in modern warfare.

In his book, Keir Giles discuss cyber and information warfare strategies deployed by Russia against Ukraine (Giles, 2023). It highlights how Russia's holistic and integrated approach to information warfare has both validated and contradicted previous assessments of its military capabilities. The paper underscores the importance for future victims of Russian aggression to understand the interdependencies between cyber, information, physical, and cognitive domains. Additionally, it discusses the role of private industry and international partners in Ukraine's resilience, the legal implications of civilian involvement in wartime information activities, and provides policy recommendations to bolster resilience against similar threats from state and non-state actors

While significant research has explored the cyber warfare tactics used in the Russia-Ukraine conflict, gaps remain in understanding the broader technical implications and potential strategic utilization of commercial technologies like SpaceX's Starlink. Existing studies, like those by Dr. Herbert Lin and Marcus Willet, provide valuable insights into immediate cyber operations and Ukrainian resilience, highlighting critical infrastructure disruptions and the role of international support. However, these analyses often overlook the strategic consequences of integrating commercial satellite systems into national defense frameworks. Itzhak Aviv's work emphasizes communication infrastructure vulnerabilities and Starlink's role, but it doesn't delve deeply into the strategic implications or potential applications in other geopolitical contexts, including for non-state actors. Similarly, Keir Giles' research on Russian cyber and information warfare strategies underscores the interconnectedness of cyber and information domains but lacks a focused analysis on the transformative impact of commercial satellite networks. This research seeks to address this gap by examining Starlink's role in critical infrastructure protection and its strategic consequences in cyber warfare. Using the Ukraine-Russia conflict as a case study and exploring potential utilization by Papuan separatist groups, this study will offer a thorough understanding of the implications of commercial satellite technology in modern conflict scenarios and its potential for future applications by both state and non-state actors.

3. Research Methodology

3.1. Qualitative Research Thematic Synthesis Method

Qualitative research thematic synthesis method is a method used to collect, organize, and analyze data from various qualitative studies that focus on a particular topic or theme (Thomas & Harden, 2008). This method includes several stages: searching, quality assessment, and data extraction from studies, with detailed procedures for thematic synthesis. As shown in Figure 1 below.

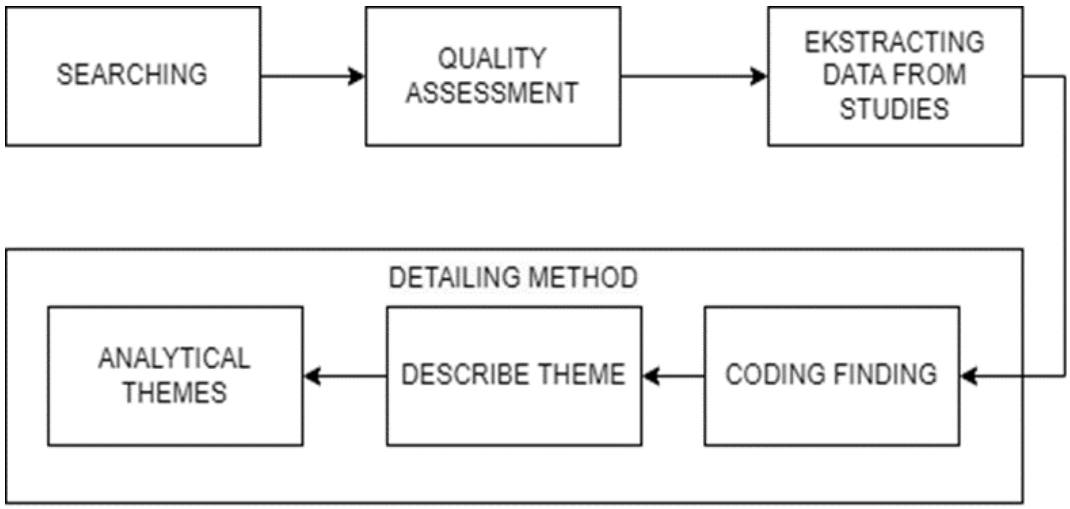

Figure 1. Flow of thematic synthesis research method.

Following is the explanation of the qualitative research thematic synthesis method:

3.1.1. Searching

The first stage is to identify and collect qualitative studies relevant to the research topic. This involves systematically searching the literature in various academic databases, journals, and other sources that can provide the necessary data.

3.1.2. Quality Assessment

After collecting the studies, the next step is to assess the quality of each study to ensure that only high-quality research is included in the synthesis. This was done using predetermined assessment criteria to assess the validity, reliability and relevance of the studies.

3.1.3. Extracting Data from Studies

This stage involves extracting key information from each study. Extracted data included key findings, direct quotes from participants, study context, and authors' interpretations. This information was then organized to facilitate further analysis.

3.1.4. Detailed Methods for Thematic Synthesis

The methods section of a manuscript describes the research methods. Authors must clearly describe the research methodology for transparency and replicability.

3.1.4.1. Coding Findings

At this stage, data extracted from previous studies is coded. Coding is a process in which similar or related data are given specific labels or marks to identify emerging themes or patterns.

3.1.4.2. Describe Theme

After coding, the next step was to group similar codes into broader themes. Each theme is thoroughly described to highlight the relevant findings and their connection to the research questions.

3.1.4.3. Analytical Themes

The final stage was to develop analytical themes from the identified themes. This involves in-depth analysis to identify relationships between the themes and generate new, more comprehensive insights into the research topic. These analytical themes often contribute significantly to a more in-depth and theoretical understanding of the phenomenon under study.

3.2. Method Justification

That this research method, which is thematic synthesis, has been used in research on intelligence analysis themes such as a study about the Russian-Ukraine armed conflict (Aviv & Ferri, 2023). This research has indeed been widely discussed by defense experts in the European Union and beyond. However, this research is still not related to the conflict in Papua. Therefore, the theme that we raise is a new theme and is expected to make a major contribution to military intelligence research in the Southeast Asian region.

3.3. Research Limitation

This research aims to explore the conflict from two main points of view. First, the technical dimension which includes the military technology and strategy used, secondly the military dimension which focuses on field tactics and operations. In this analysis, the research specifically avoids discussing the socio-political aspects of the conflict, with a more focused focus on a deep understanding of the technical and strategic dynamics that influenced the development of the conflict.

4. Research Thematic Synthesis

4.1. Searching

We search for various references related to the study about Russian-Ukrainian war that have direct or indirect relation with the usage of modern communication devices such as satellite-based internet connection. We take references from various sources such as journals, conferences, research article publications. Up-to-date military and technology news is also become our source of information. The main

tool that we use for the search is google scholar search engine. In this stage, we could at least extract information from around 50 articles with around 30 technical articles becoming our main source of ideas to look for potential security risks.

4.2. Quality Assessment

The criteria's to choose relevant sources are:

1) Relatively recent studies with a publication year above 2010, and

2) References that have an explicit relevance to the subject matter of this study (Russian-Ukrainian war and the technical impact of satellite-based communication unit).

4.3. Data Extraction

In this stage, we run our process based on subsection 4.1. and uses the quality assessment criteria from section 4.2. From around 50 plus research articles and news related to Russian-Ukrainian war and the usage of satellite-based communication system, based on the quality assessment criteria, we got at least 30 technical papers that have good quality and relevance to the technology background used by satellite-based communication system. The rest 20 of the articles are used to construct the warfare related ideas.

4.4. Theme Synthesis

This stage try to combine the three substages: coding findings, describe themes, and analytical themes in one direct process. The substage of coding findings leverages a tool called Researchrabbit to create a relation based reference graph like shown in Figure 2. Inside those graph, there are many references or articles with the same theme. We try to analyze all of the main ideas of related papers to synthesis research theme.

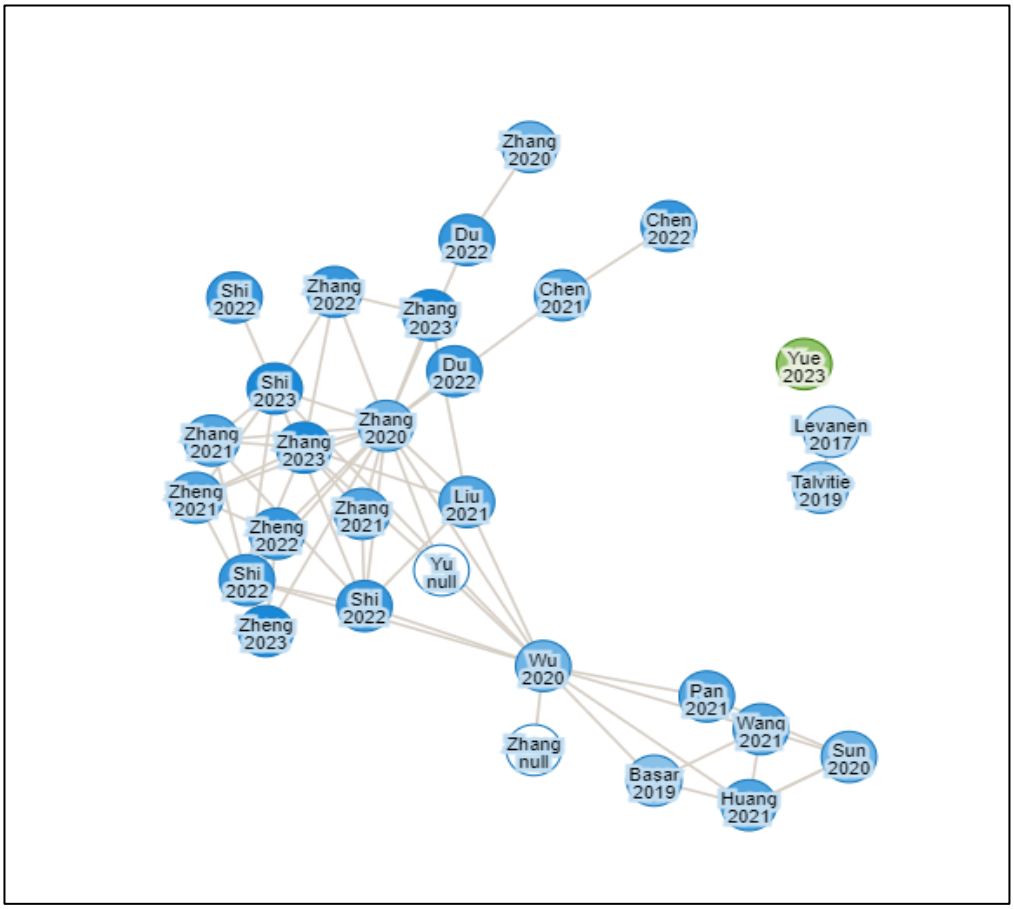

Figure 2. Researchrabbit reference graph.

4.4.1. Initial Exploration and Literature Review

We began with a comprehensive literature review to identify the security and reliability challenges of Low Earth Orbit (LEO) satellites. Initial studies highlighted the vulnerabilities and necessary security measures for these satellite communication systems, setting the stage for our deeper exploration (Yue et al., 2023). This paper highlighted the vulnerabilities in satellite communication systems, which became a central theme in our subsequent analysis. Simultaneously, we examined advancements in related communication technologies, such as 5G networks for high-speed railways, which provided insights into integrating advanced communication systems in dynamic environments (Levanen et al., 2017; Talvitie et al., 2019).

4.4.2. Deep Dive into Intelligent Communication Systems

A significant portion of our research focused on Reconfigurable Intelligent Surfaces (RIS) and their impact on communication systems. Studies on RIS-assisted wireless communications and protocols for high-mobility scenarios provided critical insights into mitigating issues like Doppler effects and multipath fading (Huang et al., 2021; Sun & Yan, 2021). These findings were crucial for understanding how RIS could enhance satellite communication performance in dynamic and high-mobility environments, relevant to both military operations in Ukraine and potential separatist activities in West Papua.

4.4.3. Application to High-Stakes Environments

The practical application of these advanced communication technologies was explored through case studies involving high-mobility vehicular communication (Basar, 2021; Wang et al., 2021). These studies offered a practical perspective on implementing RIS in scenarios requiring high mobility and reliability, drawing parallels to military applications and highlighting the potential operational advantages for both state and non-state actors.

4.4.4. Cybersecurity and Strategic Implications

Understanding the cybersecurity aspects was paramount. Research on signal processing techniques and security measures for RIS-assisted systems provided a detailed look at the cybersecurity risks and mitigation strategies necessary for the effective deployment of these technologies (Pan et al., 2022; Ren et al., 2023). These insights were directly applicable to understanding the cybersecurity risks associated with Starlink and similar technologies in conflict zones.

4.4.5. Synthesis and Thematic Development

Through synthesis, we identified critical themes and strategic implications. Research highlighted the transformative potential of these technologies, providing a framework for understanding their strategic implications in military conflicts (Zhang et al., 2020, 2021).

The intersection of these technologies with real-world applications was further explored through research papers that talk about High-Speed Train Communications and Wireless Energy Transfer via MIMO Systems (Shi et al., 2022; Zheng et al., 2022). These studies underscored the potential of advanced communication technologies to enhance operational capabilities in conflict zones, providing a basis for our case study of the Ukraine-Russia conflict and potential utilization by the Papuan separatist groups.

4.4.6. Conclusion and Future Directions

By synthesizing diverse research findings, we concluded that the theme "Starlink in the Context of Critical Infrastructure Protection and Strategic Consequences in Cyber Warfare" is both timely and critically important. The Ukraine-Russia conflict demonstrated the strategic advantages and cybersecurity risks associated with advanced satellite communication systems. By extrapolating these findings to the context of the Papuan separatist groups, we identified potential scenarios and strategic implications, contributing to the broader understanding of modern cyber warfare and infrastructure protection.

5. Result and Discussion

5.1. Starlink Overview

Starlink is a satellite constellation developed by SpaceX to deliver high-speed internet access globally, especially in areas with limited terrestrial infrastructure, such as rural areas. It uses low Earth orbit (LEO) satellites equipped with advanced technologies like phase array antennas and laser communication to

deliver high-speed internet with low latency. Starlink aims to bridge digital connectivity gaps by offering reliable internet services where traditional methods are economically impractical or insufficient, thereby supporting educational and economic activities on a more equitable basis worldwide. Since SpaceX deployed its first set of Starlink constellation satellites in May 2019, concerns have arisen within the astronomical community regarding potential disruptions to astronomical observations.

The usefulness of starlink has dismissed concerns that the large LEO satellite constellation could adversely affect astronomy and pose risks to specific orbits. There is no doubt that the world's need for affordable and equitable internet connectivity is high. Take Starlink's offer of free internet to emergency responders and the Hoh Tribe in Washington, for example. However, it is important to realize that it is not the free internet offer that is the business and goal of starlink, but there are missions and visions that must be watched together (Rawls et al., 2020).

As an initial look, Starlink is a revolutionary satellite-based internet service developed by SpaceX under the leadership of Elon Musk, which has significantly changed global internet access. The system works by transmitting data signals between multiple LEO satellites in orbit and gateway stations on the ground. As of February 2024 in its report Starlink mentions that SpaceX has begun controlled deorbit on 406 satellites out of nearly 6000 Starlink satellites launched (Starlink, 2024). In Indonesia, the presence of Starlink still triggers several challenges, ranging from regulatory aspects, data sovereignty, operator business sustainability, social environmental and cultural impacts, and space junk issues (Lisnawati, 2024).

In its mission to provide low-latency global connectivity, starlink operates the world's largest constellation of satellites in the world, with a rapidly growing user base in 37 countries and growing (Starlink, 2022). For instance, countries like Lithuania boast an average download speed of 160 Mbps, while in the US it is 91 Mbps, in Canada 97 Mbps, and in Australia 124 Mbps. The Mexican region tops the list with the fastest average download speed of 105.91 Mbps (Cooper, 2023).

To support these internet speeds, the starlink satellite is at an altitude of Low Earth Orbit (LEO). With this altitude the internet problem in remote areas will be resolved. Figure 3 below shows a comparison picture of the vision between satellites at LEO altitude, MEO, and GEO.

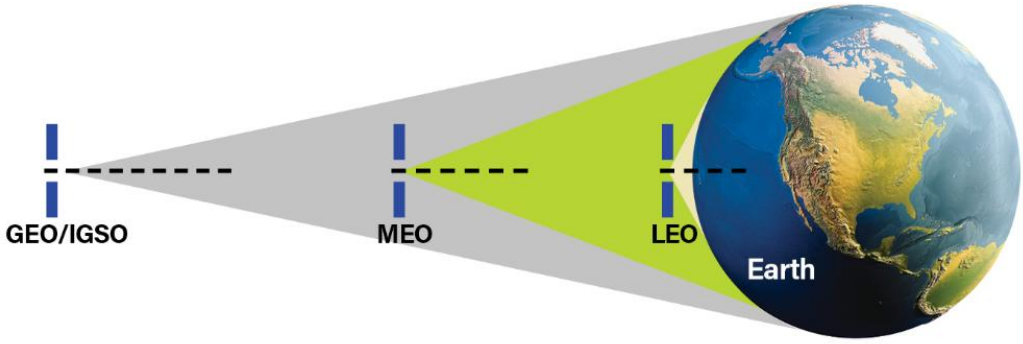

Figure 3. Field of view: Satellites in LEO, MEO, and GEO.

Source: www.airandspaceforces.com

Unlike traditional satellite internet services that rely on Geostationary Earth Orbit (GEO) and Medium Earth Orbit (MEO) satellites, Starlink's LEO satellites operate at altitudes spanning from approximately 160 km to 2,000 km above Earth, with most of its satellites positioned around 550 km. This relatively low altitude is a key factor in the system's performance and distinguishes it significantly from MEO and GEO satellites.

GEO satellites, are positioned in a geostationary orbit, maintaining a fixed position relative to a point on Earth's surface. This allows for continuous coverage of a specific area with a single satellite, which is advantageous for certain applications like television broadcasting and weather monitoring. However, the high latency and lower bandwidth efficiency associated with GEO satellites make them less suitable for high-speed internet services.

LEO satellites in the other hand, due to their proximity to Earth, offer several notable advantages. One of the primary benefits is reduced latency. For LEO satellites like those in the Starlink network, the latency can be as low as 20 to 40 milliseconds, which is on par with many terrestrial broadband services. This low latency is particularly advantageous for applications requiring real-time interaction. Traditional GEO satellites, orbiting at around 35,786 km above Earth, typically have a latency of about 600 milliseconds due to the greater distance signals must travel. This makes real-time applications challenging with GEO satellites, highlighting a significant edge for LEO systems.

Furthermore, the lower altitude of LEO satellites translates to higher data throughput and improved bandwidth efficiency. Signals traveling to and from LEO satellites experience less attenuation and path loss compared to those communicating with satellites in higher orbits. This results in stronger and clearer signals, enabling faster data transmission speeds. Consequently, LEO satellite networks can support a higher number of users with greater data demands, which is increasingly important as the global need for broadband internet continues to grow.

Another advantage of LEO satellites is their ability to provide ubiquitous coverage, even in remote and underserved areas. Traditional terrestrial broadband infrastructure is often economically unfeasible to deploy in sparsely populated or geographically challenging regions. LEO satellites, by contrast, can blanket the entire planet, ensuring that even the most isolated communities have access to reliable internet. This feature of Starlink's service holds significant implications for narrowing the digital divide and promoting increased global connectivity.

However, the operation of LEO satellite constellations comes with its own set of challenges and disadvantages. One significant challenge is the need for a large number of satellites to ensure continuous coverage. Unlike GEO satellites, which stationary relative to a fixed point on Earth, LEO satellites move quickly across the sky, completing an orbit in about 90 to 120 minutes. To maintain uninterrupted service, a dense network of satellites is required so that as one satellite moves out of range, another is available to take its place. This necessitates a substantial investment in satellite production, deployment, and maintenance.

The rapid movement of LEO satellites also necessitates sophisticated tracking and handoff mechanisms. User terminals and ground stations must be capable of seamlessly switching connections from one satellite to another without service interruptions. This adds complexity to the system design and requires advanced technology to manage the constant changes in satellite positions and signal paths.

Another potential disadvantage of LEO satellite networks is their shorter operational lifespan compared to GEO satellites. LEO satellites are subjected to higher levels of atmospheric drag due to their lower altitudes, leading to a gradual decay of their orbits. As a result, LEO satellites typically have a lifespan of around five to ten years, compared to the 15 to 20 years common for GEO satellites. This shorter lifespan necessitates regular replacement and replenishment of the satellite constellation, adding to the long-term operational costs.

Despite these challenges, the advantages of LEO satellites, particularly in the context of internet connectivity, often outweigh the disadvantages. When compared to MEO and GEO satellites, LEO satellites provide superior performance in terms of latency, bandwidth efficiency, and global coverage. MEO satellites, orbiting at altitudes between 2,000 km and 35,786 km, offer a middle ground in terms of latency and coverage. They have lower latency than GEO satellites but higher than LEO satellites. However, MEO satellites still need fewer satellites to cover the same geographical scope compared to LEO, which can be an advantage in terms of deployment and maintenance.

In conclusion, the concept of LEO satellites as implemented by Starlink offers a compelling solution for global internet connectivity. The low latency, high data throughput, and ability to provide ubiquitous coverage make LEO satellites particularly well-suited for modern internet applications. While there are challenges associated with deploying and maintaining a large constellation of LEO satellites, the benefits they offer in terms of performance and accessibility are significant. Compared to MEO and GEO satellites, LEO satellites provide a better balance of latency, coverage, and bandwidth efficiency, making them a superior choice for delivering internet to users around the world. As the demand for reliable and fast internet continues to grow, the role of LEO satellites in meeting this demand is likely to become increasingly important, potentially transforming the landscape of global communications.

5.2. Starlink Timeline and History

5.2.1. Conception and Early Development (2015-2018)

Starlink's origins can be traced back to 2015 when SpaceX first publicly disclosed plans for a satellite internet constellation (Kalyani, 2021). Elon Musk envisioned a global network that could deliver high-speed internet access to underserved and remote areas worldwide. Initial discussions within SpaceX centered around leveraging advances in satellite technology, including miniaturization, mass production, and reusable rocket technology, to lower the cost of deploying and maintaining a satellite constellation. By early 2016, SpaceX had filed regulatory documents with the Federal Communications Commission (FCC) outlining plans for a constellation of approximately 4,000 satellites operating in multiple orbital planes at altitudes between 1,110 km and 1,325 km. The ambitious scope of the project aimed to provide low-latency, high-bandwidth internet coverage globally, rivaling or surpassing existing terrestrial broadband networks in terms of speed and reliability. The following years saw intensive research and development efforts at SpaceX's facilities in Hawthorne, California, focusing on satellite design, propulsion systems, inter-satellite communication links, and ground infrastructure. SpaceX engineers iteratively improved satellite components to enhance performance, minimize weight, and maximize operational lifespan, while simultaneously developing advanced antenna technologies for user terminals on the ground.

5.2.2. Prototype Testing and Regulatory Hurdles (2019-2020)

In 2019, SpaceX launched the first batch of experimental Starlink satellites, named Tintin A and Tintin B, aboard a Falcon 9 rocket. These satellites served as prototypes to validate key technologies and demonstrate the feasibility of the planned constellation architecture (Shaengchart & Kraiwanit, 2023). Successful testing of these prototypes paved the way for subsequent launches and regulatory approvals necessary for full-scale deployment. Regulatory challenges emerged as SpaceX navigated international spectrum allocation rules and coordination requirements with other satellite operators and governmental bodies. In the United States, SpaceX obtained regulatory approvals from the FCC for initial satellite deployments and spectrum use, while concurrently engaging with international regulators to secure authorizations for global coverage. Throughout 2020, SpaceX accelerated its launch cadence, deploying batches of operational Starlink satellites aboard Falcon 9 rockets. Each launch campaign aimed to steadily expand the constellation's coverage and capacity, focusing initially on regions with high demand for improved internet connectivity, such as rural and remote areas lacking reliable terrestrial broadband options.

5.2.3. Expansion and Operational Deployment (2021-2023)

The year 2021 marked a significant milestone for Starlink as SpaceX ramped up production and deployment efforts. Improved satellite designs, including upgrades to enhance performance and reliability, were incorporated based on insights gained from earlier launches and operational feedback (Herath, 2021). SpaceX continued to refine ground infrastructure, deploying user terminals and gateway facilities to facilitate seamless integration with the satellite constellation.

By mid-2021, Starlink began offering commercial internet services to select regions under a beta testing program known as "Better Than Nothing Beta." This phase allowed early adopters to experience Starlink's capabilities firsthand, providing valuable feedback to optimize service quality and user experience. As customer demand surged, SpaceX expanded its manufacturing capabilities and accelerated satellite production to meet deployment targets. By early 2022, Starlink surpassed significant milestones, including the deployment of over 2,000 operational satellites and the provision of broadband services to tens of thousands of customers across multiple countries. Operational challenges, including regulatory compliance, spectrum management, and orbital debris mitigation, remained focal points as Starlink continued its global expansion. SpaceX collaborated with regulatory authorities and international organizations to address concerns related to satellite interference, orbital congestion, and environmental impact, demonstrating a commitment to responsible space utilization and sustainability.

5.2.4. Future Prospects and Beyond (2024 and Beyond)

Looking ahead, Starlink's trajectory involves further expanding coverage, enhancing service reliability, and lowering costs to make broadband internet more accessible globally. SpaceX plans to deploy additional satellites, implement technological advancements, and refine operational processes to scale the network efficiently. Innovative developments such as laser inter-satellite links (ISLs) promise to enhance network performance by enabling direct satellite-to-satellite communication, reducing latency and improving data

transmission speeds. These advancements align with SpaceX's broader vision to establish a self-sustaining space-based ecosystem capable of supporting future missions to Mars and beyond. The integration of Starship, SpaceX's next-generation spacecraft, into satellite deployment strategies could potentially streamline operations and reduce launch costs further. Starship's ability to carry larger payloads and facilitate rapid, cost-effective deployment of satellite constellations may accelerate Starlink's growth trajectory and enhance its competitive edge in the global telecommunications market. Moreover, Starlink aims to play a pivotal role in bridging the digital divide, particularly in underserved regions lacking reliable internet infrastructure. By providing affordable, high-speed broadband connectivity, Starlink seeks to empower communities, stimulate economic development, and foster educational opportunities worldwide. In conclusion, Starlink represents a paradigm shift in satellite communications, leveraging cutting-edge technology and innovative business strategies to redefine global internet connectivity. From its inception to ongoing deployment and future aspirations, SpaceX's commitment to advancing space-based telecommunications underscores its role as a pioneer in the aerospace industry, with Starlink poised to shape the future of digital connectivity on a global scale.

5.3. Starlink Usage in the Ukraine-Russia Conflict

Internet via satellite was first used for military purposes in the 1960s and became available for wide-scale commercial use in the 1990s (Evans et al., 2011). Satellite internet was first utilized for military purposes in the 1960s, marked by the deployment of early communication satellites like SCORE (Signal Communications by Orbiting Relay Equipment) for relaying voice and data. Significant advancements included the MILSTAR (Military Strategic and Tactical Relay) and DSCS (Defense Satellite Communications System) systems, which provided secure and anti-jam communications for the U.S. military.

During the Vietnam War, satellites such as SYNCOM III (Synchronous Communications) enhanced operational coordination. The Gulf War in the 1990s saw extensive use of satellite communications for real-time coordination of coalition forces. Additionally, the GPS, initially developed for military navigation, became fully operational in the 1990s, offering precise positioning and timing essential for military operations.

These military applications laid the groundwork for the widespread commercial use of satellite internet in the 1990s. The emergence of cybersecurity risks targeting satellite communications is a recent development that has rapidly become a major concern for the ongoing viability of satellite networks. These risks target critical vulnerabilities that could have detrimental effects, including compromising launch systems, communication channels, telemetry, tracking, command operations, and the overall mission success. Secure and resilient cyber capabilities are essential throughout the entire lifecycle of a satellite to ensure the integrity of these vital components (Housen-Couriel, 2016).

A large portion of global focus on the utilization of space during Russia's conflict in Ukraine, especially concerning commercial space services, has emphasized satellite capabilities, neglecting the importance of other elements of space systems like ground infrastructure, software, and practices for sharing information (Dziwisz & Sajduk, 2023). While Russia possesses a multitude of military satellites and Ukraine has none, international and commercial collaboration in space information sharing, along with advancements in terrestrial hardware and software, have enabled Ukraine to surpass Russia in utilizing space across operational, strategic, and diplomatic domains (Öztemel, 2022). Ukraine and its allies have effectively demonstrated the strategic advantages of their networked, distributed approach to utilizing and sharing space-based information. This contrasts with Russia's centralized command structure, which has struggled to gather and disseminate timely satellite intelligence to its forces.

Space systems are composed of three essential components: the space segment, which includes the operational satellites; the ground segment, encompassing Earth-based systems, operators, and data processing facilities; and the link segment, which consists of the communication signals connecting satellites to each other and to ground users and operators. Each segment is crucial for data acquisition and distribution, and neglecting any part reduces the effectiveness of the entire system (see Fig. 4).

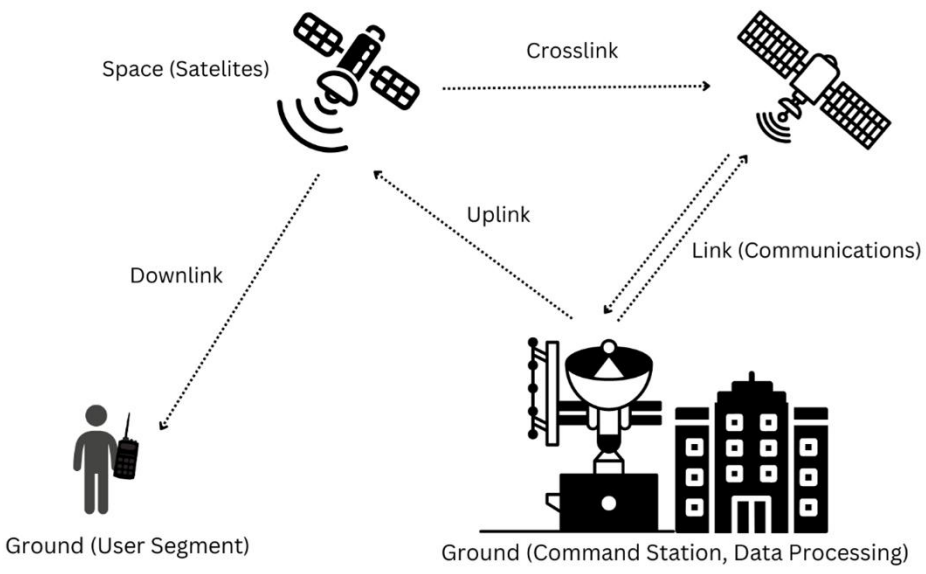

Figure 4. Space system segments.

At the beginning of the Russian invasion, Ukraine lacked its own satellites and operational infrastructure. However, the United States, NATO Allies, and commercial entities stepped in to provide extensive support through various space services. This assistance has allowed Ukraine to utilize space systems to a much greater extent than anticipated, considering its limited capabilities before February 2022, when independent access to space was not available. While the focus has been on Ukraine's effective use of commercial space services in tactical situations, these space-based systems have also had significant operational and strategic impacts.

Ukraine relies on satellite services provided by the US military, particularly GPS signals crucial for precision in rockets, bombs, and artillery used by its forces. GPS has long been a NATO standard for Positioning, Navigation, and Timing (PNT). In addition, commercial remote-sensing satellites, capable of high-resolution electro-optical and Synthetic Aperture Radar (SAR) imagery, play a vital role. SAR imagery is especially valuable in low-visibility conditions like nighttime or cloudy weather. These commercial satellites assist in tracking Russian troop movements and buildups in Ukraine, Russia, and Belarus. The availability of diverse imagery has enabled Ukraine to precisely locate, monitor, and target Russian forces before strikes and assess damage afterward, thereby improving ammunition efficiency and operational effectiveness. Commercial companies such as Maxar, Planet, and BlackSky have directly contributed to this activity. Ukraine utilizes various commercial satellite communication (SATCOM) systems for diverse purposes. During the initial days of the conflict, Ukrainian President Volodymyr Zelensky maintained regular communication with the United States while on the move, using a secure satellite phone provided by the White House before the invasion. Companies like Iridium, Globalstar, and Inmarsat offer capabilities in this sector. Zelensky also employs Starlink satellites to communicate directly with Ukrainians, national parliaments, and international organizations worldwide. These commercial telecom satellites enable continuous connectivity among Ukrainians and provide critical services such as emergency internet and phone services to refugee camps along the Ukrainian border, facilitated by Luxembourg-based satellite operator SES.

Starlink plays a pivotal role by offering broadband internet across Ukraine, supporting both military and civilian users and contributing significantly to Ukraine’s battlefield achievements. The connectivity provided by Starlink facilitates secure communication and enhances situational awareness from high-ranking officials to command centers and frontline units, enabling effective coordination in various military operations.

Other commercial satellite companies, such as SES, Eutelsat, OneWeb, Inmarsat, Iridium, Viasat, and Avanti, also offer internet connectivity to Ukraine from space. Viasat, OneWeb, and SES are actively enhancing their capacity through new satellite constellations and agreements with Ukrainian telecom

operators. Despite these efforts, Starlink continues to be the primary provider of mobile satellite communication services in Ukraine, maintaining a prominent presence.

One reason Starlink has been widely adopted at the tactical level is due to its compact antennas, approximately the size of a pizza box, which are smaller than those of many other commercial satellite systems. This portability makes them easily transportable by mobile, tactical teams. At the individual unit level, Ukrainian forces have utilized Starlink to transmit real-time drone video feeds directly to artillery batteries. This capability enables artillery units to precisely observe where their rounds land and make necessary adjustments to their fire. Additionally, reconnaissance drones using Starlink satellite relays have facilitated coordination among ground forces, including directing soldiers armed with shoulder-fired antitank weapons to strategic positions for attacks. Attack drones that directly target Russian tanks, positions, and other objectives are also enabled by Starlink.

The Russian cyberattack on Viasat in February 2022 exploited a vulnerability in ground systems, effectively denying Ukrainian forces access to crucial space capabilities. This attack disrupted global navigation satellite system (GNSS) signals, impacting targeting, troop coordination, and potentially affecting air travel, logistics, and essential services. Despite Russia's attempts to jam Starlink satellites, operators have successfully adapted their code to mitigate the interference.

While several commercial satellite firms support Russia's military operations, Russia utilizes commercial space capabilities less extensively compared to Ukraine and its allies. This is partly because many commercial companies have restricted Russia's access to their services due to sanctions imposed by the United States and others. Additionally, Russia's military structure is not conducive to adopting the decentralized, networked approach favoured by these commercial technologies.

Ukraine has demonstrated that the effective utilization of satellite data and services depends not only on their availability but also on how efficiently they are delivered to the war fighter. In April 2023, then-Major General David Miller, who served as director of operations, training, and force development for US Space Command, emphasized that warning, surveillance, and targeting information holds little value if it cannot reach the end-user. Moreover, the skills, motivation, and innovative tactics of war fighters themselves amplify the effectiveness of space capabilities, as evidenced by Ukrainian forces' successful utilization of space resources (Dickey & Gleason, 2024).

5.4. Potential Utilization of Starlink by West Papuan KKB

Given the increasing use of Starlink in Indonesia, concerns have arisen regarding its potential misuse by groups such as the KKB (Kelompok Kriminal Bersenjata). KKB Papua, or the West Papua Liberation Army, is an armed separatist group operating in the provinces of Papua and West Papua, Indonesia (Hafiz & Pratama, 2021). Emerging from unresolved historical grievances dating back to Papua's integration into Indonesia in 1969, KKB has conducted a range of militant activities aimed at challenging Indonesian authority. These activities include armed skirmishes, hostage-taking, demonstrations, and symbolic gestures such as raising the Morning Star flag, a symbol of Papuan independence (Effendi & Panjaitan, 2021).

KKB's actions have significantly disrupted local governance and security, particularly in areas like Biak Numfor, Sorong, Paniai, and beyond, often exploiting porous border controls to facilitate movement and logistics. Despite occasional political reforms allowing for greater expression of Papuan identity and aspirations since the late 1990s, KKB's persistence underscores ongoing challenges in achieving lasting peace and reconciliation in Papua (Sianturi & Hanita, 2020).

If KKB were to harness Starlink's capabilities, it could significantly enhance their operational efficiency, posing a substantial threat to regional security. The portability and reliability of Starlink's compact antennas would enable the KKB to maintain robust communication across remote and rugged terrains, facilitating real-time coordination and strategic planning. This scenario mirrors the military advantages seen in Ukraine, where Starlink's high-speed internet has bolstered battlefield communications and situational awareness. The potential for KKB to leverage such technology raises alarms about increased insurgency capabilities, making it imperative for Indonesian authorities to monitor and regulate access to these satellite services carefully.

5.5. Strategy Development for Starlink Utilization

5.5.1. Potential Risks

5.5.1.1. Battleground Capability Risks

In the context of the ongoing conflict between West Papuan separatist groups known as KKB, and the Indonesian government, parallels can be drawn from the use of Starlink by Ukraine during the Russia-Ukraine conflict to explore potential warfare scenarios where these separatist groups might leverage similar satellite communication technologies for strategic advantages such as:

1) **Mobile Communication Hubs**: The KKB could use Starlink's portable satellite antennas to establish mobile communication hubs. This would allow for secure and reliable communication among dispersed units in remote and mountainous terrains where traditional communication infrastructure is either inadequate or has been destroyed. The ability to coordinate and command in real-time, much like the Ukrainian forces do, would enable the KKB to relay instructions and synchronize their movements effectively, enhancing their military operational capabilities.

2) **Integration with Reconnaissance Drones**: Integrating Starlink with reconnaissance drones could provide the KKB with real-time intelligence on Indonesian military movements, allowing them to make informed strategic decisions. This mirrors how Ukrainian forces used drone video feeds for precise targeting and artillery fire adjustments. These drones could be transferred from bordering Nations that have potential adversity with Indonesian government such as Papua New Guinea.

3) **Public Relations**: On the public relations front, leveraging Starlink's global reach could enable KKB leaders to broadcast messages to international audiences, appealing for support and highlighting their cause, akin to Ukrainian President Volodymyr Zelensky's communications with global leaders and citizens during the conflict.

4) **Cybersecurity and Resilience**: If Indonesian cyber operations were to target KKB's communications, Starlink’s adaptable software could offer resilience. For instance, if Indonesia attempted to jam satellite signals, Starlink’s operators could update the system’s code to counteract these efforts, like the measures taken to mitigate Russian interference in Ukraine.

5) **Resource Allocation**: The precise positioning and navigation capabilities of Starlink could also help the KKB optimize their resource allocation by accurately tracking the movement of their forces and supplies, thereby reducing waste and improving logistical efficiency, like how Ukraine utilized GPS for precision strikes and resource management.

Strategically, access to advanced satellite communication technologies would significantly enhance the operational capabilities of the KKB, posing a greater challenge to Indonesian military and cyber forces. Effective use of such technologies could also draw international attention and potentially entice sympathy or support from external entities, complicating Indonesia's efforts to manage the conflict.

This scenario underscores the critical importance of cybersecurity measures for satellite communication systems, as any vulnerabilities could be exploited, leading to significant strategic consequences, much like the ViaSat cyberattack during the Ukraine-Russia conflict. The potential use of Starlink by West Papuan separatist groups thus illustrates the transformative impact of satellite communication technologies in modern conflicts, highlighting the need for robust cybersecurity measures and strategic foresight from all involved parties.

5.5.1.2. Cyberspace Operational Risks

The deployment of Starlink in conflict zones especially by the Indonesian Armed Forces in the mid of a battleground presents several cybersecurity risks like described by Figure 5, including but not limited to:

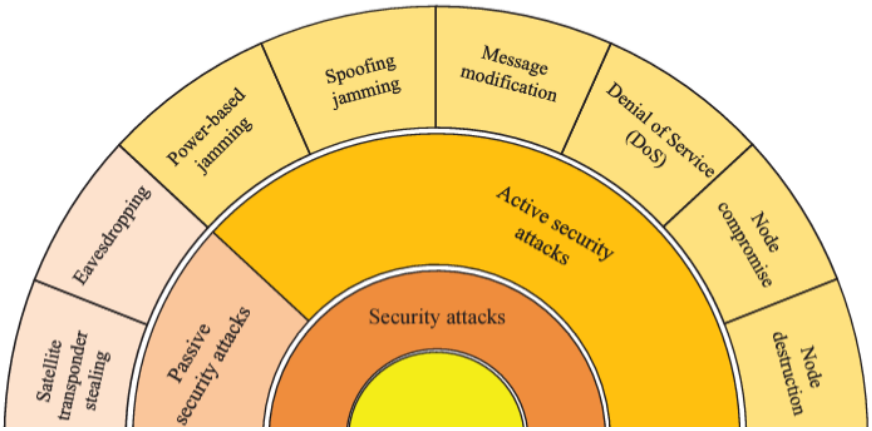

Figure 5. Cyberspace operational risk.

1) **Signal Interception and Jamming**: Adversaries which is in this case KKB could intercept or jam the Indonesian Starlink interconnecting signals, disrupting communication and possibly could be extended into an intelligence gathering operation. In this scenario, the intruder could prevent information transmission that later could endanger the uninformed Indonesian Army position.

2) **Eavesdropping/Surveillance**: The open characteristic of wireless connection makes data transmission easily vulnerable to the interception. Using the same reasoning, sensitive data transmitted via Starlink interconnection could be intercepted by cyber adversaries, leading to potential leaks of strategic information. Furthermore, the modification of transmitted messages could endanger the Indonesian Armed Forces operation and even mislead them into doing bad decisions.

3) **System Destruction or Manipulation**: Unauthorized access to Starlink systems, especially the user-side terminal device could allow adversaries to manipulate satellite operations, potentially rerouting data or disabling services.

4) **Spoofing Attacks:** Cyber adversaries might conduct spoofing attacks. The attacker tricks receiver to believe that the malicious signal produced by the attacker is legitimate. The feeding of false information to Starlink-enabled devices could be done by the attacker and could lead to misinformed strategic decisions.

5) **Denial of Service (DoS) Attack**: An attacker attempt to shut down a server or network, making it inaccessible to its intended users by flooding it with huge amount of traffic. A DoS attack usually occur in the ground and space segment of LEO.

5.5.2. Counterintelligence Strategies

5.5.2.1. Battleground Mitigation

To overcome both Battleground Capability Risks and Cyberspace Operational Risks, immediate action needs to be taken. This urgency is further supported by the fact that Indonesian Armed Forces are currently still fighting the KKB in the jungle of West Papua. Here are possible counterintelligence strategies that could be implemented in the field to face the challenge of Starlink usage by KKB and its associates:

1) **Limiting Access**: Restricting access to Starlink devices for the West Papuan Separation Army through stringent control measures and surveillance. This strategy includes the effort to increase monitoring capabilities around the Indonesian eastern national border to limit the weapon, device, and even human resource smuggling operation.

2) **Frontline usage limitation**: The use of Starlink on the frontlines raises concerns about operational security and the potential exposure of military strategies and movements. Some potential risks such as communication jamming, device destruction, device acquisition, and eavesdropping. The solution to these problems is to limit the usage of Starlink interconnection in

the frontline of the battlefield. It is better to use more specific and secure channels to communicate between allies.

3) **Device Modification**: Implementing device modifications to prevent spoofing and eavesdropping. Ensuring that frontline units do not rely solely on Starlink default configuration for critical communications to mitigate risks of interception.

4) **Infrastructure Support**: The geolocation and navigation capabilities provided by Starlink could enhance logistical support, ensuring efficient resource distribution and movement coordination. Also, the reliability of Starlink devices against weather conditions and the ability to stay in communication as long as there is a nearby Ground Station Unit make it worth it to provide one or more Ground Station Unit relatively close to the warzone.

5) **Secure Data Relays**: Ensuring that all data relays only pass through Indonesian Ground Stations to monitor and control the flow of information and prevent unauthorized access.

In summary, the utilization of Starlink by Papuan separatist groups presents both significant advantages and substantial risks. To counteract these, a multifaceted strategy involving stringent cybersecurity measures, counterintelligence operations, and controlled access to communication infrastructure is essential. The insights drawn from the Russia-Ukraine conflict provide a valuable framework for understanding and mitigating these risks in the context of Indonesia's security landscape.

5.5.2.2. Strategic Mitigation

In response to the potential risks posed by the adoption of Starlink technology by groups like Indonesia's Papuan separatist KKB (Kelompok Kriminal Bersenjata), the Indonesian government faces critical decisions regarding regulatory and security measures. Given the transformative impact of satellite communication technologies in modern conflicts, Indonesia must prioritize robust cybersecurity frameworks to safeguard against misuse and potential threats to national security. This entails establishing stringent regulations governing the acquisition, deployment, and operation of satellite communication systems within Indonesian territory.

Firstly, Indonesia should develop comprehensive policies that require thorough vetting and licensing procedures for satellite service providers like Starlink. These regulations should ensure that operators comply with national security standards, including encryption protocols and cyber resilience measures, to prevent unauthorized access or interference. Collaborating with international stakeholders and regulatory bodies can provide insights into best practices and ensure alignment with global cybersecurity standards. Secondly, continuous monitoring and surveillance capabilities should be implemented to detect and respond swiftly to any suspicious activities or potential breaches involving satellite communications. This includes investing in advanced cybersecurity infrastructure capable of detecting and mitigating cyber threats in real-time, particularly those targeting critical infrastructure and communications networks. Furthermore, enhancing national cybersecurity capabilities through training programs and partnerships with cybersecurity experts will be crucial. These efforts should focus on building indigenous expertise in satellite communications security, including threat assessment, incident response, and forensic investigation, to strengthen Indonesia's defense against cyber-attacks and unauthorized use of satellite technologies. In parallel, fostering international cooperation and information sharing agreements with satellite service providers and other nations will be essential. This collaborative approach can facilitate intelligence gathering on emerging threats and enhance Indonesia's ability to respond effectively to evolving cybersecurity challenges in the satellite communications domain. Ultimately, by adopting a proactive stance on cybersecurity and regulatory oversight of satellite communication technologies, Indonesia can mitigate potential risks associated with their misuse by groups like the KKB. This approach not only safeguards national security interests but also promotes responsible and secure utilization of advanced satellite technologies for societal benefit and economic development.

The physical location of a Network Operation Center (NOC) within Indonesia's borders is imperative for Starlink, enabling BSSN, Indonesia's National Cyber and Crypto Agency, to deploy crucial sensors for monitoring network traffic and detecting anomalies. This setup ensures real-time detection and response to cybersecurity threats, crucially safeguarding the integrity and security of Starlink's operations in the country.

Starlink is mandated by Indonesia's Personal Data Protection Law (UU PDP) to enforce robust encryption protocols and data security standards, ensuring protection of user data exchanged or stored within the country. Regulation No. 8 of 2023 issued by BSSN outlines comprehensive frameworks that Starlink must strictly adhere to, particularly in securing ground stations, gateway operations, and network communications within Indonesian territory.

Before commencing operations, Starlink must fully comply with telecommunications regulations stipulated by BSSN and other governmental bodies, ensuring alignment with national security standards and critical infrastructure protection guidelines. It is critical to establish a dedicated Computer Security Incident Response Team (CSIRT) registered with BSSN to bolster readiness against potential cyber incidents through effective incident detection, response, mitigation, and recovery strategies.

Operational readiness tests overseen by the Ministry of Communication and Information Technology (Kominfo) verify that Starlink's devices and infrastructure meet the stringent standards required for operating as a VSAT operator and ISP in Indonesia, validating technical capabilities, network reliability, and compliance with regulatory mandates. Starlink's use of local IP addresses, provided by authorized local internet gateway providers, ensures that all internet traffic is routed through local infrastructure, meeting stringent national security and operational requirements.

While initial operations may rely on remote engineering support, Starlink remains committed to building a local workforce in Indonesia, recruiting engineers and customer service personnel to bolster operations, resolve technical issues promptly, and enhance overall customer satisfaction. Tailoring gateway configurations in border regions such as Singapore guarantees seamless connectivity for Indonesian users, compliant with local regulatory frameworks and optimizing network performance and reliability.

Kominfo exercises oversight over Starlink's operations through a dedicated task force in collaboration with BSSN, ensuring adherence to regulatory requirements and swift resolution of emerging issues in telecommunications and satellite services. Conducting a Proof of Concept (PoC) assessment with the Directorate of Control of the Directorate General of Post and Informatics (Dirjen PPI) validates that Starlink's operations conform to legal frameworks governing telecommunications, data security, and vital information infrastructure protection in Indonesia, ensuring full compliance prior to operational deployment.

6. Conclusion

6.1. Lesson Learned

This study try to highlights the critical impact of Starlink technology usage in the Ukraine-Russia conflict, where Starlink has proven its ability to maintain communications stability amidst the disruption of conventional infrastructure due to military attacks. Ukraine's use of Starlink has enabled the government and military to maintain effective coordination and operations, as well as provide reliable internet access for affected civilians. The technology has become a key element in Ukraine's cyber defense strategy, demonstrating how satellite communications solutions can overcome the limitations of ground networks in crisis situations.

The potential utilization of Starlink by the KKB (Kelompok Kriminal Bersenjata) in Papua is also a key concern in this research. Access to high-speed internet connection supported by Starlink could provide a strategic advantage to the KKB, allowing them to strengthen operational coordination, spread propaganda, and enhance intelligence capabilities without being easily detected by the Indonesian government. This poses new challenges for national security, as the KKB's ability to operate secure, encrypted communications could complicate law enforcement efforts and threaten stability in the region.

To manage and oversee the use of Starlink, the development of a comprehensive utilization strategy is necessary. This includes establishing a Network Operations Center (NOC) to monitor network activities, ensuring compliance with the Personal Data Protection Law (PDP Law), and establishing a Computer Security Incident Response Team (CSIRT) specialized in handling cyber incidents. In addition, operational readiness and operational readiness tests should be conducted regularly to ensure rapid response to threats. Collaboration between National Cyber and Crypto Agency (BSSN), Ministry of Communication and Information Technology (Kominfo), Starlink, Association of Indonesian Internet Service Providers (APJII),

and Internet Service Providers (ISPs) is also essential to create an integrated and effective security ecosystem. With the right strategy, the benefits of Starlink can be optimized while minimizing possible risks to national security.

6.2. Future Work

Even though risk mitigation strategies for using Starlink-based internet in the battlefield of West Papua have been provided, the enemy still has the potential to counter these strategies. Firstly, when access restrictions are implemented along the eastern border of Indonesia with Papua New Guinea to curb the smuggling of weapons, soldiers, and Starlink devices, it is possible that Papua New Guinea's allies may protest at the United Nations Assembly. Secondly, when efforts are made to implement comprehensive national cybersecurity strategies through policy development, there may be parties that hinder these plans. These obstacles can come from both domestic and international sources, motivated by various interests, including financial gain, political agendas, and geopolitical strategies. Therefore, further research is needed to prepare strategies to face these challenges and obstacles.

References

Amanda, M. R., & Pramono, B. (2023). Resolusi Konflik Kelompok Kriminal Bersenjata Papua. *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam*, *5*(1), 971–984. https://doi.org/10.37680/almanhaj.v5i1.2855

Aviv, I., & Ferri, U. (2023). Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem. *International Journal of Critical Infrastructure Protection*, *43*, 100637. https://doi.org/https://doi.org/10.1016/j.ijcip.2023.100637

Basar, E. (2021). Reconfigurable Intelligent Surfaces for Doppler Effect and Multipath Fading Mitigation. *Frontiers in Communications and Networks*, *2*. https://doi.org/10.3389/frcmn.2021.672857

Cooper, T. (2023). *Starlink Availability Map*. https://broadbandnow.com/starlink#

Dickey, R., & Gleason, M. P. (2024). *Spacepower and Strategy: SPACE AND WAR IN UKRAINE Beyond the Satellites*. https://bbc.com/.

Dziwisz, D., & Sajduk, B. (2023). The Russia-Ukraine Conflict from 2014 to 2023 and the Significance of a Strategic Victory in Cyberspace. *Applied Cybersecurity & Internet Governance*, *2*(1), 1–20. https://doi.org/10.60097/acig/162842

Effendi, T., & Panjaitan, A. C. D. (2021). KONSEKUENSI PENETAPAN STATUS KELOMPOK KRIMINAL BERSENJATA (KKB) DALAM KONFLIK PAPUA SEBAGAI GERAKAN TERORIS MENURUT HUKUM PIDANA. *Rechtidee*, *16*(2), 223–245. https://doi.org/10.21107/ri.v16i2.11823

European Space Policy Institute. (2022). *The War in Ukraine from a Space Cybersecurity Perspective*. www.espi.or.at

Evans, B. G., Thompson, P. T., Corazza, G. E., Vanelli-Coralli, A., & Candreva, E. A. (2011). 1945-2010: 65 years of satellite history from early visions to latest missions. In *Proceedings of the IEEE* (Vol. 99, Issue 11, pp. 1840–1857). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/JPROC.2011.2159467

Giles, K. (2023). *Russian cyber and information warfare in practice Lessons observed from the war on Ukraine*.

Hafiz, M., & Pratama, S. M. (2021). *TINJAUAN HUKUM PENETAPAN KELOMPOK KRIMINAL BERSENJATA PAPUA SEBAGAI TERORIS DALAM PERSPEKTIF HUKUM PIDANA NASIONAL* (Vol. 7, Issue 1). Online. https://www.kompas.id/baca/polhuk/2021/04

Herath, H. M. V. R. (2021). *Starlink : A Solution to the Digital Connectivity Divide in Education in the Global South*.

Housen-Couriel, D. (2016). Cybersecurity threats to satellite communications: Towards a typology of state actor responses. *Acta Astronautica*, *128*, 409–415. https://doi.org/10.1016/j.actaastro.2016.07.041

Huang, Z., Zheng, B., & Zhang, R. (2021). Transforming Fading Channel from Fast to Slow: IRS-Assisted High-Mobility Communication. *ICC 2021 - IEEE International Conference on Communications*, 1–6. https://doi.org/10.1109/ICC42927.2021.9500699

Ismail, M. (2015). Strategi Pengembangan Ekonomi Rakyat di Provinsi Papua. *Jurnal Bina Praja*, *7*(3), 251–260. https://doi.org/10.21787/jbp.07.2015.251-259

Kalyani, P. (2021). "Internet From Sky: Starlink", An Empirical Study on The Introductory Offer from Starlink In Pandemic Situation-Its Competition, Opportunity and Future in one of the world's biggest consumer Market-India. *Journal of Management Engineering and Information Technology (JMEIT)*, *8*. https://doi.org/10.5281/zenodo.4733198

Kraz. (2024). *STARLINK "BERBAHAYA" BAGI INDONESIA*. https://investigasinusantara.com/starlinkberbahayabagi-indonesia/

Levanen, T., Talvitie, J., Wichman, R., Syrjälä, V., Renfors, M., & Valkama, M. (2017). Location-aware 5G communications and Doppler compensation for high-speed train networks. *2017 European Conference on Networks and Communications (EuCNC)*, 1–6. https://doi.org/10.1109/EuCNC.2017.7980755

Lin, H. (2022). Russian Cyber Operations in the Invasion of Ukraine. *The Cyber Defense Review*, *7*(4), 31–46. https://www.jstor.org/stable/48703290

Lisnawati. (2024). KEHADIRAN STARLINK DI INDONESIA: MANFAAT DAN DAMPAK. *Infosingkat*, *Vol. XVI*(No. 11/I/Pusaka/Juni/2024).

Ogden, T., Knack, A., Lebret, M., Black, J., & Mavroudis, V. (2024). *The Role of the Space Domain in the Russia-Ukraine War The impact of converging space and AI technologies*.

Öztemel, İ. Ş. (2022). Digital Hegemony and the Russia-Ukraine War. *İletişim ve Diplomasi*, *8*, 43–57. https://doi.org/10.54722/iletisimvediplomasi.1124928

Pan, C., Zhou, G., Zhi, K., Hong, S., Wu, T., Pan, Y., Ren, H., Renzo, M. D., Swindlehurst, A. L., Zhang, R., & Zhang, A. Y. (2022). An Overview of Signal Processing Techniques for RIS/IRS-Aided Wireless Systems. *IEEE Journal of Selected Topics in Signal Processing*, *16*(5), 883–917. https://doi.org/10.1109/JSTSP.2022.3195671

Rawls, M. L., Thiemann, H. B., Chemin, V., Walkowicz, L., Peel, M. W., & Grange, Y. G. (2020). Satellite Constellation Internet Affordability and Need. *Research Notes of the AAS*, *4*(10), 189. https://doi.org/10.3847/2515-5172/abc48e

Ren, S., Shen, K., Zhang, Y., Li, X., Chen, X., & Luo, Z.-Q. (2023). Configuring Intelligent Reflecting Surface with Performance Guarantees: Blind Beamforming. *IEEE Transactions on Wireless Communications*, *22*. https://doi.org/10.1109/TWC.2022.3217679

Rosyid, F. A. (2020). ANALISIS DAMPAK INVESTASI TERHADAP PEREKONOMIAN DAERAH: STUDI KASUS INVESTASI PERTAMBANGAN MINERAL LOGAM PROVINSI PAPUA. *Indonesian Mining Professionals Journal*, *2*(1), 11–28. https://doi.org/10.36986/impj.v2i1.18

Santika, E. F. (2024). Tingkat Penetrasi dan Kontribusi Internet Indonesia berdasarkan Pulau (2024). *Databoks*.

Setiawan, W. (2017). Era Digital dan Tantangannya. *Seminar Nasional Pendidikan*.

Shaengchart, Y., & Kraiwanit, T. (2023). PUBLIC PERCEPTION OF THE STARLINK SATELLITE PROJECT IN A DEVELOPING COUNTRY. *Corporate and Business Strategy Review*, *4*(3), 66–73. https://doi.org/10.22495/cbsrv4i3art7

Shaengchart, Y., & Kraiwanit, T. (2024). THE SPACEX STARLINK SATELLITE PROJECT: BUSINESS STRATEGIES AND PERSPECTIVES. *Corporate and Business Strategy Review*, *5*(1), 30–37. https://doi.org/10.22495/cbsrv5i1art3

Shi, E., Zhang, J., Chen, S., Zheng, J., Zhang, Y., Ng, D. W. K., & Ai, B. (2022). Wireless Energy Transfer in RIS-Aided Cell-Free Massive MIMO Systems: Opportunities and Challenges. *IEEE Communications Magazine*, *60*(3), 26–32. https://doi.org/10.1109/MCOM.001.2100671

Sianturi, B. H., & Hanita, M. (2020). Optimalisasi Peran Polri Dalam Penanganan Kelompok Kriminal Bersenjata di Papua (Optimizing the Role of the National Police in Handling Armed Criminal Groups in Papua). In *Jurnal Keamanan Nasional: Vol. VI* (Issue 1).

Starlink. (2022). *STARLINK WELCOMES SECURITY RESEARCHERS (BRING ON THE BUGS)*. https://www.starlink.com/updates

Starlink. (2024). *Commitment to Space Sustainability*. https://www.starlink.com/updates

Sun, S., & Yan, H. (2021). Channel Estimation for Reconfigurable Intelligent Surface-Assisted Wireless Communications Considering Doppler Effect. *IEEE Wireless Communications Letters*, *10*(4), 790–794. https://doi.org/10.1109/LWC.2020.3044004

Talvitie, J., Levanen, T., Koivisto, M., Ihalainen, T., Pajukoski, K., & Valkama, M. (2019). Positioning and Location-Aware Communications for Modern Railways with 5G New Radio. *IEEE Communications Magazine*, *57*(9), 24–30. https://doi.org/10.1109/MCOM.001.1800954

Thomas, J., & Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC Medical Research Methodology*, *8*. https://doi.org/10.1186/1471-2288-8-45

Urbanus Panggabean, J., Anwar, S., & Ppn, K. (2023). The Role of Russian Cyber Operations in The Russian-Ukraine War in Achieving Russia's Strategic Objectives. *The Indonesian Journal of Development Planning*, *VIII*(1), 118–131. https://doi.org/10.36574/jpp.v8i1.470

Wang, K., Lam, C.-T., & Ng, B. K. (2021). IRS-aided Predictable High-Mobility Vehicular Communication with Doppler Effect Mitigation. *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, 1–6. https://doi.org/10.1109/VTC2021-Spring51267.2021.9448955

Willett, M. (2022). The Cyber Dimension of the Russia–Ukraine War. *Survival*, *64*(5), 7–26. https://doi.org/10.1080/00396338.2022.2126193

Yue, P., An, J., Zhang, J., Ye, J., Pan, G., Wang, S., Xiao, P., & Hanzo, L. (2023). Low Earth Orbit Satellite Security and Reliability: Issues, Solutions, and the Road Ahead. *IEEE Communications Surveys & Tutorials*, *25*(3), 1604–1652. https://doi.org/10.1109/COMST.2023.3296160

Zhang, J., Björnson, E., Matthaiou, M., Ng, D. W. K., Yang, H., & Love, D. J. (2020). Prospective Multiple Antenna Technologies for Beyond 5G. *IEEE Journal on Selected Areas in Communications*, *38*(8), 1637–1660. https://doi.org/10.1109/JSAC.2020.3000826

Zhang, J., Liu, H., Wu, Q., Jin, Y., Chen, Y., Ai, B., Jin, S., & Cui, T. J. (2021). RIS-Aided Next-Generation High-Speed Train Communications: Challenges, Solutions, and Future Directions. *IEEE Wireless Communications*, *28*(6), 145–151. https://doi.org/10.1109/MWC.001.2100170

Zheng, J., Zhang, J., Björnson, E., Li, Z., & Ai, B. (2022). Cell-Free Massive MIMO-OFDM for High-Speed Train Communications. *IEEE Journal on Selected Areas in Communications*, *40*(10), 2823–2839. https://doi.org/10.1109/JSAC.2022.3196088