iCOBEST
International Conference on Business Economics, Social Sciences & Humanities

UNIKOM

STRATEGIC ANALYSIS OF ISRAEL AND HEZBOLLAH'S HYBRID WARFARE: A CASE STUDY OF PAGER AND WALKIE-TALKIE SABOTAGE

Regina Rivera Rafa Dany
Universitas Komputer Indonesia, Bandung, Indonesia

M Rivaldi Naufal
Universitas Komputer Indonesia, Bandung, Indonesia

N Merlin Cahyawati
Universitas Komputer Indonesia, Bandung, Indonesia

M. Farhan Rasyidi
Universitas Komputer Indonesia, Bandung, Indonesia

Dewi Triwahyuni
Universitas Komputer Indonesia, Bandung, Indonesia

ABSTRACT

This research aims to understand the hybrid war between Israel and Hezbollah and provide an empirical analysis of its war strategy based on a specific case. The method used in this research is qualitative through a descriptive approach to explain the phenomenon of Israel's attack in September 2024. In its development, cyberspace has become one of the actors in the world of international relations, which impacts the global dynamics of relations between countries. Hence, the concept of hybrid warfare carried out by Israel and Hezbollah is a research that must be studied further. The results of this study show that Israel's hybrid warfare strategy, exemplified by the 2024 sabotage of Hezbollah's pagers and walkie-talkies, represents a significant evolution in modern conflict, combining cyber and physical tactics to exploit vulnerabilities, disrupt enemy operations, and create psychological impacts. This approach not only escalates tensions between Israel and Hezbollah but also poses new challenges for international law, regional security, and conflict resolution, highlighting the growing complexity of hybrid warfare in contemporary international relations. This research advances insights into hybrid warfare, guides policymaking on cyber-physical security, underscores legal and diplomatic challenges, and promotes further research into its psychological and societal effects.

Keywords: Communication System Hacking, Hezbollah, Hybrid Warfare, Israel, War Strategy

INTRODUCTION

Hybrid warfare in the Israel-Hezbollah conflict case manifests as a blend of traditional military assault and cyber attacks, including hacking (Solmaz, T. 2022). According to the geographical map, Israel and Lebanon are two countries that share a direct border and are historically linked; they share a complex relationship that deteriorated after Israel ended the relationship and established a border that could not be crossed as freely as before. Then, in 1982, Israel's establishment in 1948 and its 1982 invasion of South Lebanon. This conflict continues today (Yulianto, M. A. 2013). During Lebanon's civil war, Hezbollah emerged as a powerful Iranian-backed militant group opposing Israel and Western influence. Hezbollah, defined as the "party of God," over time, has become a non-state actor that has a substantial impact on the government of Lebanon (crf.org editor. 2024). As mentioned in the book "Lebanon Pre- and Post-War 34 Days Israel vs .Hezbollah", one resident of South Lebanon claims that no one has won in this conflict, and both sides declare their victory. The conflict between Lebanon and Israel is best portrayed as two brothers constantly retaliating against each other —each strike provokes a counter-strike, creating an endless cycle of violence. As a result, the conflict between these two countries continues and has never been resolved until now. One of the cases that caught the author's attention was the event behind the hacking of Hezbollah's pagers and walkie-talkies in September 2024. If you look back, this hack did not just happen immediately; some factors triggered this operation, and of course, there was a long process before Israel succeeded in hacking Hezbollah.

Previous studies on the Israel-Hezbollah conflict and hybrid warfare have provided valuable insights from various perspectives, laying the groundwork for this research on Strategic Analysis of Israel vs Hezbollah Hybrid Warfare: A Case Study of Pager and Walkie-Talkie Sabotage. Hendrianto's research (2021) examines Israel's cybersecurity strategies, emphasizing its efforts to develop advanced cyber capabilities for maintaining national security and forming international coalitions in the Middle East. However, this study extends Hendrianto's work by analyzing Israel's targeted cyber operations against Hezbollah in 2024, particularly the sabotage of pagers and walkie-talkies, offering a more detailed examination of hybrid warfare tactics. C. Sheng et al. (2024) provide a technical analysis of physical cyber-attacks, focusing on vulnerabilities of communication devices like pagers and walkie-talkies and then proposing cybersecurity improvements to cybersecurity protocols. Still, this research diverges by emphasizing the strategic motivations behind the sabotage, framing it within hybrid warfare rather than the purely technical. Aurelie Daher's work (2024) connects Hezbollah's activities to broader regional dynamics, particularly its role in supporting Palestine during the October 7, 2023, Hamas attack on Israel, reinforcing the interconnectedness of hybrid warfare tactics as part of a more significant strategic response to regional threats. Yasmine Khayyat's article (2025) and her broader work in the book provide a civilian perspective on the enduring societal impact of the Israel-Lebanon conflict, focusing on the lived experiences of those affected by the war. This research complements Khayyat's work by shifting the focus to the strategic and military dimensions of the 2024 sabotage, integrating cybersecurity, regional dynamics, and civilian impacts into a comprehensive analysis of hybrid warfare. Unlike previous studies, this research emphasizes the strategic motivations and outcomes of the attack, offering a unique perspective on the evolving nature of the Israel-Hezbollah conflict and the role of hybrid warfare in modern conflicts.

The purpose of this research is to provide a strategic analysis of the Israel-Hezbollah hybrid warfare, with a specific focus on the 2024 event, sabotage of Hezbollah's pagers and walkie-talkies as a case study. By examining this event through a qualitative and interpretive lens, the study aims to uncover the underlying motivations, strategies, and broader implications of hybrid warfare in modern conflicts. This research contributes to the existing literature by offering a varied understanding of how cyber operations are integrated into hybrid warfare tactics, particularly in the Israel-Hezbollah conflict, and how such actions influence regional dynamics. The author's knowledge is derived from internet-based data collection, analysis of news reports, and interpretive reasoning, emphasizing the socially constructed nature of reality and the importance of intersubjectivity in understanding complex phenomena. Through storytelling and narrative analysis, the study contributes to contextualizing the phenomena. It enriches the discourse on hybrid warfare and its evolving role in modern conflicts, not only highlighting the strategic dimensions of sabotage.

LITERATURE REVIEW

The Concept of Hybrid Warfare

When academics or practitioners mention a hybrid warfare model, it does not always imply the same meaning, especially if we explore the definitions by institutions and countries, each with its concept (Solmaz, T. 2022). Many researchers still perceive the idea of hybrid warfare as quite ambiguous and controversial (Caliskan, M., & Liégeois, M. 2020). The word 'Hybrid' in hybrid warfare describes the fusion of more than one form or dimension of force to attack the opponent's weaknesses while reducing the opponent's deployed strength. Therefore, this definition causes confusion in which the limits of hybrid warfare are questioned because it is asymmetrical and thus difficult to measure (Reichborn-Kjennerud, E., & Cullen, P. 2022). This concept is widely criticized because it causes uncertainty in its definition, which is too broad, causing general vagueness. However, it is a concept that has existed for a long time, and the packaging of hybrid warfare is still new and considered an immature concept (Kaldor, M. 2013). For Dr. Chris Tuck, hybrid warfare reflects our fear of an uncertain future and the non-traditional threats that come with it. When there is a consciousness towards insecurity, there is a perception of new threats that may occur, and this leads to the multiplication of the threat's image and encourages a race to increase power, which aggravates the danger through the view of hybrid warfare to infinity.

Regardless, each country or organization understands and defines the hybrid concept in its own way. To establish a clear conceptual framework, the author narrows down the idea of hybrid warfare based on Frank Hoffman's definition, as he is one of the key researchers who popularized the term hybrid war through his monograph. Hoffman emphasizes the importance of understanding the historical and cultural context that led to the beginning of the conflict to classify the war into the hybrid category (Hoffman, F. G. 2007). He explicitly defines hybrid warfare as multiple modes of warfare, including conventional forces, unarticulated tactics and formations, terrorist acts, including violence and coercion, and criminal interference. In the context of hybrid warfare between Israel-Hezbollah, hybrid warfare manifests as a blend of conventional military attacks and cyber operations through hacking (Solmaz, T. 2022). This approach combines traditional techniques and capabilities with unconventional skill sets and performs them simultaneously in the same battle space (Reichborn-Kjennerud, E., & Cullen, P. 2022). ATG's defining characteristic of hybrid warfare is its fusion of conventional military tactics with irregular combat, cyberattacks, and information operations, which collectively pose significant challenges to national security (Sarjito, A. 2024).

The concept of International Security

In the study of international relations, “national security” refers to the state's responsibility to protect its sovereignty, territorial integrity, and security from external and internal threats. In the modern world, national security includes military, technological, economic, political, and social elements (Buzan, 1991). Military resilience is essential to national security and refers to a country's ability to defend itself against external threats through military readiness, technological advancement, and innovative strategies (Waltz. 1979). In its conflict with Hezbollah, Israel has employed hybrid warfare, utilizing unconventional tactics to undermine its opponent's capability. For instance, Israel leveraged technological resilience to protect its national security by sabotaging Hezbollah walkie-talkies and pagers.

Hybrid Warfare blurs the line between conventional and unconventional warfare, as demonstrated by Israel's strategic attacks on Hezbollah's communication systems. These actions show that simple technological vulnerabilities can transformed into potent, dangerous weapons when exploited effectively. Israel's military resilience is evident in its ability to adapt and conduct highly effective operations with minimal losses. Recognizing communication and information systems as critical infrastructure vulnerabilities, Israel targeted Hezbollah's device as part of a broader defense strategy, showcasing its capacity to understand and exploit the opponent's weaknesses (Liberman. 2006). Israel has developed a dynamic and unpredictable defense strategy by combining conventional military tactics with irregular methods. The sabotage of Hezbollah 's communication device exemplifies Israel's efficiency in preempting threats, narrowing the enemy's operating space, and creating strategic uncertainty. This demonstrates how robust military resilience, grounded in technological dominance and innovative strategies, can enhance national security by anticipating and neutralizing threats in advance (Synder. 2021).

Cybersecurity Theory

Cyber security has emerged as a modern global security cornerstone; it is considered a technical aspect that requires protection and a strategic battleground that includes asymmetric warfare and extensive psychological damage. Cybersecurity experts, such as Nye (2010), emphasize that information security, especially in the cyber context, depends not only on technological devices but also on the dynamics of interactions between states that utilize cyberspace for geopolitical purposes. Given the borderless and often anonymous nature of cyber, this poses a significant challenge for international law in establishing clear principles regarding the rights and obligations of states in carrying out offensive cyber operations. In a deeper cyber analysis, the concept of cyber deterrence becomes fundamental in understanding the dynamics of cyber security. This cyber deterrence includes efforts to prevent cyber attacks by mitigating potential risks and providing a proportional response to existing threats. As explained by Libicki (2009), deterrence in the cyber context is more complex than in the traditional military dimension due to the uncertainty regarding attacks' origin and potential impact. This approach demands the development of an adaptive cyber defense infrastructure integrated within state policy, which enables states to maintain cyber resilience while avoiding unwanted conflict escalation effectively.

In the context of Israel versus Hezbollah, the case studies of pager detonation and walkie-talkie exploitation reflect how cyber operations integrate with kinetic strategies to create asymmetric advantages in armed conflict. These incidents show that cyber warfare functions in the digital space and has material implications that amplify the effectiveness of physical attacks. The detonation of pagers as a manifestation of the penetration of the enemy's communication systems shows how cyber operations can disrupt the opponent's information network, disrupt military coordination, and weaken the effectiveness of Hezbollah's guerrilla warfare tactics. Meanwhile, the manipulation of walkie-talkies as the primary medium of communication for militant groups is concrete evidence that control of the electromagnetic spectrum is not only an intelligence instrument but also a means to manipulate the dynamics of the battlefield in real-time. This phenomenon supports Arquilla and Ronfeldt's (2001) argument that information warfare allows state actors to achieve strategic goals without direct conventional forces. The Israel-Hezbollah conflict reflects the transformation of contemporary conflicts increasingly oriented toward information superiority as the primary determinant of strategic victory. In the context of international relations, cyber operation shows that power is no longer solely measured by conventional military aspects but also by the actor's ability to control information flows, manage perceptions, and exploit the vulnerability of the enemy's communication system to achieve political and security goals more subtly and with minimal direct involvement in large-scale escalation.

Balance of Power Concept

Balance of Power (BOP) is a concept in international relations that describes power distribution among states to prevent the dominance of one particular state or alliance (Chatterjee, P. 1972). The primary purpose of balance of power is to maintain stability and avoid large-scale conflicts while ensuring that no entity can control power. The concept of balance of power is often interpreted variously, both at the level of states and the international system (Haas, E. 1953). There are two types of balance of power: Simple Balance of Power and Multiple

Balance of Power. A simple balance of power only exists between two countries or groups of countries with equal power. In contrast, multiple balances of power can exist between many countries or groups of countries that balance each other.

According to Hans J. Morgenthau (1968), BOP is a policy aimed at achieving a particular state, the actual distribution of power, and a roughly balanced power distribution. Lisolette Odgaard adds that the balance of power has a function to ensure an ideal distribution of power so that no country or group of countries can dominate a particular region or resource. The advantages of the BOP system include protecting small states, creating peace through a balanced power distribution, and enforcing compliance with international law in anarchy. Its implementation challenges include the risk of war, uncertainty in power predictions, and the possibility that the system may not prevent conflict in the event of a significant change in the balance (Odgaard, L. 2007).

The conflict between Israel and Lebanon reflects the complexity of the balance of power in the Middle East (Salim, A. R. M. 2016). Iran's involvement through Hezbollah shows how regional powers can confront each other to maintain or expand their influence. Meanwhile, Israel's strategy to counter this threat creates a new dynamic that continues to evolve in regional geopolitics. The BOP concept is implementable and relevant in the modern context, despite criticism for emphasizing military power over diplomacy (Jönsson, C. 2022). States today seek to maintain balance through military alliances and strengthen their economic position, especially in a multipolar situation where several great powers compete (Muhammad, A. (2023). Tensions resulting from competition in the Middle East often lead to large-scale conflicts and political instability (Lynch, M. 2018). With conflicting interests, the Middle East's BOP affects local countries and has global implications. The concept of Balance of Power in the Middle East reflects the complex dynamics between various regional and international powers.

METHODOLOGY

This paper employs qualitative research, which conducted exploration with a descriptive approach to understand phenomena through empirically grounded reasoning (Nadirah, S. P. et al., 2022). Since the case study used in this research is a recent event, the data collection relies on an internet-based system, utilizing credible online sources such as news articles, official statements, and expert analysis, alongside interviews derived from news reports to diverse perspectives. The understanding created from this analysis is interpreted in the narrative of this research discussion. In Umar Suryadi Bakry's book, Geoff Walsham argues that our knowledge of reality results from social construction through actors. How we understand the world and share meaning together is more intersubjectivity than objectivity (Walsham, G. 2006). Interpretive research uses storytelling or narrative research to understand the context and phenomena that can provide deeper insights into the strategic motivations and outcomes of the sabotage (Bakry, U. S. 2016).

DISCUSSION

Chronology and Triggers for Israel's Detonation of Hezbollah Pagers and Walkie talkies

In recent years, tensions between Israel-Hezbollah have escalated due to mutual attacks. In the Iron Swords War, for example, Hezbollah was implicated in coordinating Hamas attacks on Israel (Abumbe, G. T., Terhile, A., & Helen, D. C. 2024). Hamas, which controls Gaza, and Hezbollah, which is based in Lebanon, have in common their opposition to Israel. Despite operating in different regions, they have the support of the same party, Iran. This often leads the two groups to coordinate or support each other in their efforts against Israel. However, Hamas and

Hezbollah do not have a cooperative (Khatib, L. 2025). Under the influence of Iran, they are indirectly one proxy that complies with the Iranian scenario.

The Hamas attack on October 7, 2023, killed around 1,200 people and also captured more than 250 people from the Israeli side (Selján, P. 2024). This attack was very unexpected and had a significant impact on Israel's existence. The capabilities of Israel's intelligence agencies, which are considered the best in the world, were questioned after this incident because they were unable to detect the attack (Barnea, A. 2024). As a result, Israel responded strongly to the attack not only by taking revenge in the Gaza region but also in other areas that are seen as a threat. Of course, Israel needs to maintain its national security and dampen so that the escalation does not continue. One form of a warning from Israel as a form of self-defense against neighboring countries to maintain its existence is to show strength to Lebanon so as not to mess around (Magramo, Kathleen., et al. 2024). On Tuesday, September 17, 2024, hundreds of pagers owned by Hezbollah exploded throughout Lebanon; this happened one day after Israeli officials said they would increase attacks on the group; explosions occurred in various places such as on sidewalks, grocery stores, cars, and homes, killing at least 30 people and thousands more were injured. At 3:30 pm, the pager received an incoming message ostensibly from a Hezbollah leader and beeped for several seconds. People at the scene also testified to seeing smoke coming out of Hezbollah fighters' pockets before the explosion. (Stahl, L., Aliza, C., Shachar B., Jinsol J. 2024)

The reason Hezbollah uses pagers instead of modern communication tools is because they are reliable in places with poor internet connectivity, have a long battery life that can last for days without charging, and communication using pagers is more efficient, less likely to be tracked, and can operate on specific frequencies that are harder for authorities to monitor. These devices are considered too stupid to be hacked in this increasingly sophisticated world (Akhtar, Noureen. 2024). Unfortunately, Israel saw this as an opening to launch an attack. Israel began drafting its attack scenario by making adjustments to their pagers and submitting their product to be manufactured by one of the companies from which Hezbollah purchased pagers for its operations. These pager modifications were done so subtly that Hezbollah was unaware. According to Lebanese sources, the agents who made the pagers designed batteries that are invisible to X-rays, with direct knowledge of the pagers and photos of the battery pack disassembly seen by Haaretz. (2024).

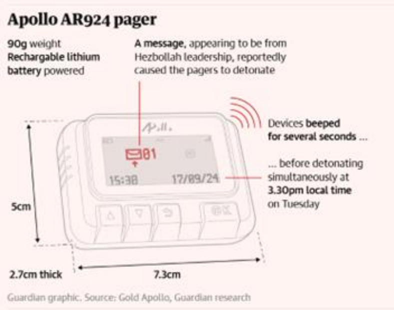
It did not stop with the pager explosion. The next day, in the atmosphere of mourning after the pager explosion and at the funeral of the victims, the tragedy occurred again on Hezbollah's walkie-talkie communication device (Moore, Marcus. 2024). This is a form of assertion by Israel. Israel does not aim to cause as many casualties as possible but rather to symbolize through the surviving victims not to underestimate Israel's power, let alone interfere with affairs in the Gaza Strip and the Lebanese border. In addition, by hacking into the communications system, Israel may have aimed to disrupt Hezbollah's coordination and command, both attacks reducing the likelihood of a counterattack or further escalation (Sarker, P.P. et al. 2025). This is part of Israel's strategy to maintain national security and prevent regional conflict. Israel also intends to tell the world that its power is more significant than what can be predicted, and the strategy devised by the people behind the scenes is not messing around and is even very outside the box. If they can hack and weaken their opponents with something as simple as pagers and walkie-talkies, imagine what they can do with more modern technology. Furthermore, not only did this incident cause physical casualties, but many sources reported that the entire civilian community was traumatized by the electronics around them and became more vigilant afterward.

If cybercrime has been defined as stealing confidential information, spying, or disabling a system from functioning, it is now much broader in scope. This implies that it is also important in cybersecurity to safeguard the physical system of the device being used, not just the network, information, and privacy (Sarker, P.P. et al. 2025). It is important to realize that cyberspace has opened up new levels that further blur the boundaries between the real and virtual spheres. Imagine what more sophisticated devices and other Internet of things are capable of if it takes outside-the-box thinking to hack into something as simple as pagers and walkie-talkies. Transformation occurs when cyber threats have reached the expression of physical impact. (Akhtar, Noureen. 2024).

War Strategy

The realist approach to international relations views hybrid warfare as a natural outcome of power competition in an anarchic global system. As rational actors, states face strategic uncertainty and competition, pushing them to adopt unconventional methods like cyber sabotage and technological infiltration to maximize their interests and strengthen their position. In an environment where survival and security are paramount, states use hybrid tactics to address power imbalances and avoid high-risk escalation. As Mearsheimer (2001) explains in The Tragedy of Great Power Politics, great powers seek dominance through military means and by manipulating non-military elements to destabilize rivals subtly (Mearsheimer, J. 2001). Hybrid warfare also reflects the security dilemma intensified by technological globalization. States no longer rely solely on conventional military power but use technology-based strategies with significant destructive potential for covert operations. Waltz (1979), in Theory of International Politics, argues that in the absence of a global authority, states develop offensive capabilities to protect their interests and counter threats (Waltz, K. 1979). Hybrid warfare thus becomes a rational tool for states to undermine opponents without immediate diplomatic or military repercussions. The Israel-Hezbollah conflict, exemplified by the 2024 pager and walkie-talkie sabotage, illustrates this dynamic. It highlights how states and non-state actors use asymmetric strategies in a fragmented geopolitical landscape driven by the competitive nature of the international system.

The Middle East's volatile geopolitical environment further complicates this dynamic. The September 2024 sabotage of Hezbollah's communication devices—pagers and walkie-talkies—represents a sophisticated escalation in asymmetric warfare. The explosions, triggered by specific messages, suggest that the devices were modified to act as remote detonation mechanisms. This level of technological sophistication points to the involvement of multiple actors, including intelligence agencies like Mossad and possibly the original manufacturers (Woodward, M. 2024). Such operations highlight the depth of modern intelligence efforts, where supply chains are infiltrated to achieve strategic goals. In summary, hybrid warfare responds to the anarchic international system, where states and non-state actors use unconventional tactics to gain an edge. The Israel-Hezbollah case demonstrates how technological advancements and strategic compromises in supply chains are leveraged to achieve significant operational impacts, reflecting modern conflicts' complex and competitive nature.


Apollo AR924 pager
90g weight
Rechargable lithium battery powered
A message, appearing to be from Hezbollah leadership, reportedly caused the pagers to detonate
81
15:38
17/09/24
Devices beeped for several seconds ...
... before detonating simultaneously at 3.30pm local time on Tuesday
5cm
2.7cm thick
7.3cm

Guardian graphic. Source: Gold Apollo, Guardian research

Figure 1: Hezbollah Pager Device

As shown in Figure 1, Hezbollah's pagers contained a thin six-gram sheet of Pentaerythritol Tetranitrate (PETN) plastic explosive sandwiched between two battery cells. The gap between the cells was filled with flammable material acting as a detonator. This three-layer assembly was encased in a black plastic sleeve and a metal case the size of a matchbox. Unlike traditional explosives, it lacked a cylindrical mini-detonator, relying instead on a spark within the battery pack to trigger the PETN explosion. Bomb experts noted that the explosives and wrapping occupied about a third of the device's volume, reducing its overall power despite its 35-gram weight (Haaretz, 2024).

Technically, the device used in this incident bears the brand identification of Taiwanese manufacturing company Gold Apollo, which was indirectly implicated in the incident and according to its founder, Hsu Ching-Kuang, production of the AR-924 pager model used in the attack had been subcontracted to BAC Consulting KFT, a relatively unknown Budapest-based company. This deal is said to have occurred three years before the incident, suggesting the possibility that the sabotage had been designed with long-term planning (Woodward, M. 2024). However, tracing BAC Consulting KFT further blurs the supply chain trail. The company was registered in Hungary in 2022 and shares an address with various other companies in Budapest, raising suspicions that this entity may be a shell company used to disguise its actual operations. Its chief executive, Cristiana Bársony-Arcidiacono, is identified through her LinkedIn profile as a London School of Economics (LSE) graduate with a linguistic background in Hungarian and Italian. With limited concrete information on BAC Consulting's operational activities, indications are growing that the company may have served as an intermediary layer in a broader sabotage operation, aiming to obscure the involvement of state actors or larger groups in this attack.

In an analytical article, Virpratap Vikram Singh and Emile Hokayem of the International Institute for Strategic Studies stated: "The scale, destruction, and precision of the attack suggest a sophisticated operation that was months in the making." Although Israel did not claim responsibility for the attack, few doubted that its security forces were behind the effort - remarkable because it involved thousands of devices and not just one booby-trapped phone like the one used to assassinate Hamas leader Yahya Ayyash in 1996. The tactical complexity inherent in this attack suggests that the operational planning went through a stage of careful strategic calculation, with long-term implications that could substantially alter the regional security landscape (Tobin B, 2024).

The attack on Hezbollah's communications infrastructure through sabotage of pager devices represents an evolution in hybrid warfare strategies. Cybersecurity techniques and the manipulation of information technology systems, including hacking embedded software, have become key instruments that demonstrate a significant transformation in modern warfare methods. In international relations, this incident illustrates state actors exploiting global technology supply chain vulnerabilities. The success of this operation also illustrates a fundamental flaw in the distribution of electronic devices. State and non-state actors can exploit these loopholes to carry out covert sabotage. Hardware and software modifications at the production stage expand the scope of cyber warfare. Cyber warfare is no longer limited to the exploitation of digital networks; the physical manipulation of technological infrastructure has become integral to unconventional military operations. This is evidence that parties with fewer resources and power can prevail against stronger parties in asymmetric war (Estriani, H. N., Dewanto, P. A., & Asyidiqi, H. 2023).

The line between cyber warfare and traditional military operations is blurred as communication technologies are increasingly utilized as high-precision attack vectors. In this study, state actors can target armed groups without direct involvement, relying on the infiltration of digital systems to achieve strategic objectives. However, the legitimacy of such operations must still be evaluated against the parameters of the law of armed conflict, which is determined by the intensity of the violence and the level of organization of the parties involved. Thus, the use of technology in hybrid warfare not only expands the dimensions of warfare but also presents complex challenges in enforcing international humanitarian law principles (Tobin B, 2024). The attack on Hezbollah's pager devices shows the characteristics of an operation that meets this threshold, given the scale of destruction, strategic coordination, and impact on the operational structure of the armed group. Thus, while this cyber sabotage demonstrates a high level of sophistication in hybrid warfare, its legal implications remain contentious in the context of the ethics and legality of modern warfare.

The case of Israel blowing up Hezbollah's walkie-talkies and pagers is a clear example of how hybrid strategies can be used to cripple an enemy using simple technology (Kahn, 2021). From a state resilience point of view, this case shows that national security is determined by military strength, technological mastery, and the ability to overcome unbalanced threats. For Israel, advanced military power allows them to contain threats before they develop. On the other hand, for Hezbollah, this incident is an important lesson on the importance of protection and strengthening communication technology to maintain military resilience on an increasingly complex battlefield.

Impact of Pager and Walkie-Talkie Hacking

Hacking Hezbollah's communications, mainly through pagers and walkie-talkies, provided Israel with critical intelligence advantages. By intercepting Hezbollah's communications, Israel gained real-time insights into the group's movements, tactics, and positions, enabling precise military operations. This intelligence also revealed Hezbollah's organizational structure, key leaders, and decision-making processes, allowing Israel to target high-value individuals and disrupt the group's command chain. Additionally, intercepted communications exposed Hezbollah's external alliances, aiding efforts to limit its logistical and diplomatic support. Beyond tactical gains, Israel used hacked data for psychological warfare, spreading disinformation to sow distrust and demoralize Hezbollah members, further destabilizing the group (Kahn, 2021)

The psychological impact of hacking on Hezbollah was profound. The breach created widespread insecurity and mistrust among members, who feared their communications were constantly monitored. This eroded morale, as fighters doubted the reliability of orders and questioned their leadership's ability to protect sensitive information. The spread of false information exacerbated confusion, leading to internal suspicion and potential conflicts. Hezbollah's fear of betrayal grew, with members suspecting infiltrators within their ranks. This psychological strain weakened their operational cohesion and combat effectiveness, while Israel's perceived omnipresence further demoralized the group (Smith, 2020). In response to the hacking, Hezbollah overhauled its communication strategies. The group adopted encryption and reverted to traditional methods like physical couriers to avoid interception. These changes, while improving security, slowed decision-making and operational efficiency. Hezbollah also enhanced its counterintelligence efforts, seeking to identify and neutralize threats. Tactically, the group shifted to more flexible guerrilla strategies to counter Israel's intelligence advantage. Internally, Hezbollah tightened information sharing, adhering to a "need-to-know" principle to minimize leaks (Center for Strategic Studies, 2023). These adaptations aimed to restore trust and morale while mitigating future vulnerabilities.

The hacking incident significantly escalated tensions between Israel and Hezbollah. By exploiting Hezbollah's communication vulnerabilities, Israel demonstrated its technological superiority, prompting Hezbollah to adopt more aggressive tactics. This technological and military escalation cycle prolonged the conflict as both sides sought to outmaneuver each other. The breach also heightened regional insecurity, complicating diplomatic efforts to resolve the conflict. Ultimately, the hacking underscored the evolving nature of hybrid warfare, where cyber operations amplify physical and psychological impacts, reshaping the dynamics of modern conflict (Kahn, 2021).

The Role of International Organizations and Views Under International Law

The United Nations (UN), with its objectives to maintain world peace and security, develop friendly relations between countries, and enhance cooperation in various fields such as economic, social, cultural, and humanitarian, plays a central role in handling the conflict between Israel and Hezbollah, primarily through the United Nations Interim Force in Lebanon (UNIFIL) mission. Established after Israel invaded Lebanon in 1978, UNIFIL aims to monitor ceasefires and assist the Lebanese government in maintaining security. Following the war between Israel and Hezbollah in 2006, the UN Security Council passed Resolution 1701, which expanded UNIFIL's mandate to include monitoring the cessation of hostilities and supporting the Lebanese Armed Forces (LAF) in maintaining stability in the region. (CNN Indonesia, 2024) Resolution 1701 initiated by the UN Security Council had a considerable impact on the conflict in 2006 as a ceasefire came into effect on August 14, 2006, and significantly reduced the conflict; Israel gradually withdrew its troops from Lebanon, UNIFIL was strengthened with additional troops and a broader mandate, and Hezbollah remained a significant force in Lebanon and still possessed weapons despite the ban. This resolution laid the foundation for the stability of South Lebanon, although tensions between Israel and Hezbollah remain to this day. (CNN Indonesia. 2024)

The UN does its part in international diplomacy to resolve this conflict. In the context of a hybrid war involving conventional and unconventional military tactics, such as rocket attacks by Hezbollah and airstrikes by Israel, the UN seeks to facilitate dialogue between the two sides. Challenges are present when some Security Council member states, such as the United States and the United Kingdom, show favoritism towards Israel, which can affect the effectiveness of proposed resolutions. In addition to the UN, other countries are also involved in mediation efforts. For example, Arab states such as Saudi Arabia and Egypt seek to mediate conflicts and reduce regional tensions. However, their respective political interests and existing alliances often influence their involvement. Despite the efforts of international organizations to create peace, the conflict remains intractable. Non-compliance with UN resolutions by both sides, as well as political instability in Lebanon and military support from Iran to Hezbollah, make the situation even more complex. UNIFIL often faces difficulties carrying out its mandate due to ongoing attacks and uncertainty on the ground. (Widyoseno, B. 2024)

The role of international organizations in the hybrid war between Israel and Hezbollah is critical but challenging. The UN mission through UNIFIL provides a framework for monitoring and mediation. However, long-term success will largely depend on the commitment of all parties to respect the ceasefire and engage in constructive dialog. The involvement of other countries can also influence the dynamics of this conflict, both positively and negatively. The hybrid war between Israel and Hezbollah poses significant challenges to international law, particularly International Humanitarian Law. The need to regulate these new forms of conflict is all the more urgent so that the protection of individuals can be effectively enforced (Widyoseno, B. 2024). Moreover, the involvement of international organizations such as the UN is crucial in creating a framework that can address the complexities of hybrid warfare in the future. Hybrid warfare refers to the combination of conventional and unconventional military techniques to achieve strategic objectives. In the context of the conflict between Israel and Hezbollah, hybrid warfare includes the use of tactics such as rocket attacks, information warfare, and support for paramilitary groups, which creates challenges for international law, especially International Humanitarian Law (IHL).

International Humanitarian Law is designed to protect individuals in situations of armed conflict. However, hybrid warfare often blurs the lines between war and peace and between combatants and non-combatants. This creates a legal vacuum that makes it difficult to enforce laws against violations that occur during conflict. There is an urgency to regulate hybrid warfare in the context of international law in order to provide legal certainty and protection for all parties involved. Research shows that special arrangements are needed to address new aspects of hybrid warfare, including cyber and information technology in conflict.

The conflict between Israel and Hezbollah has also caused reactions from various countries in the world, reactions to the ceasefire agreement and the attacks carried out by Israel. President Joe Biden stated that the ceasefire would protect Israel from Hezbollah, which is supported by Iran, and create an environment of calm. The US is working with France to ensure the ceasefire rules are fully implemented. The Egyptian Foreign Ministry stated that Israel's attack on Lebanon is a violation of Lebanon's sovereignty and will exacerbate the crisis in the Middle East. Egypt also expressed solidarity with Lebanon and its people and urged the UN Security Council to help stop Israel's attacks. Iran's Foreign Ministry strongly condemned Israel's military action, stating that the attack could have serious consequences for West Asia. They criticized the United States and Western countries for their silence on the attack. There are fears that a war between Israel and Hezbollah could lead to a regional conflict with dire consequences.

CONCLUSION AND RECOMMENDATION

This research produces an analysis that hybrid warfare carried out by Israel against Hezbollah's walkie-talkie pagers is a highly complex situation because of the use of hacking against a communication device; the use of cyber in attacking a country is a new actor that has emerged in international relations which significantly affects the handling of solving problems because this cyber attack cannot be accurately predicted who has become the leading actor. Israel's detonation of Hezbollah's pagers and walkie-talkies in September 2024 reflects an evolution in hybrid warfare strategies that combine conventional and unconventional military tactics. Israel successfully exploited vulnerabilities in Hezbollah's communication systems, resulting in significant physical and psychological losses for the group. Moreover, in this conflict, it can also be seen that this hybrid warfare significantly impacted not only the cybersecurity of both countries but also adversely affected the country's national security. These hacks not only disrupt Hezbollah's military operations but can also exacerbate the escalation of the conflict between Israel and Hezbollah, creating tensions that are difficult to resolve. The situation also poses new challenges to international law, threatening regional security. Although the UN has tried to deal with this conflict through diplomacy with both countries, the conflict between Israel and Hezbollah has been going on for years, so with this hybrid war, the conflict between the two countries is heating up because the impact caused is enormous. It is also expected that this conflict will continue.

The recommendations for dealing with the challenges arising from Israel's detonation of Hezbollah's pagers and walkie-talkies include several strategic steps. First, Hezbollah and other armed groups must improve communication security by adopting more secure technologies. Hezbollah members must receive training and education on cyber threats to recognize and address potential risks. On the other hand, international organizations such as the UN should strengthen diplomatic efforts to encourage dialogue between Israel and Hezbollah to reduce tensions and prevent this situation from happening again. In addition, the development of a more transparent international legal framework is also needed to regulate hybrid warfare, including the use of cyber technology in conflict, so that the protection of individuals can be effectively enforced then, multinational collaboration between countries with interests in the region is essential to create stability and prevent broader conflicts, taking into account complex geopolitical dynamics. These measures hope to reduce the risk of more significant conflict and create a safer environment in the Middle East region.

REFERENCES

Abumbe, G. T., Terhile, A., & Helen, D. C. (2024). Hamas-Israel Conflicts In Gaza And Its Implications For Middle East Stability. Global Journal of Social Sciences, 23(1), 157-178.

Arquilla, J., & Ronfeldt, D. (2001). Networks and netwars: The future of terror, crime, and militancy. Rand Corporation.

Akhtar, N. (2024). “Pagers explosions across Lebanon: Cyber Warfare’s New Lethal Frontier.” Accessed via https://moderndiplomacy.eu/2024/09/17/pagers-explosions-across-lebanon-cyber-warfares-new-lethal-frontier/

Bakry, U. S. (2016). International relations research methods. Yogyakarta: Student Library.

Barnea, A. (2024). Israeli Intelligence Was Caught Off Guard: The Hamas Attack on 7 October 2023—A Preliminary Analysis. International Journal of Intelligence and Counterintelligence, 37, 1056–1082. https://doi.org/10.1080/08850607.2024.2315546.

Caliskan, M., & Liégeois, M. (2020). The concept of “hybrid warfare” undermines NATO’s strategic thinking: insights from interviews with NATO officials. Small Wars & Insurgencies, 1–25. doi:10.1080/09592318.2020.1860374

CFR.org Editor. (2024). “Backgrounder: What is Hezbollah?". Accessed via https://www.cfr.org/backgrounder/what-hezbollah#chapter-title-0-2 on January 20, 2025

Chatterjee, P. (1972). The Classical Balance of Power Theory. Journal of Peace Research, 9, 51–61. https://doi.org/10.1177/002234337200900104.

CNN Indonesia. (2024). "Israel Invades Lebanon, Where Is the Position of the UN UNIFIL Peacekeepers?". Accessed via https://www.cnnindonesia.com/internasional/20241001144702-120-1150381/israel-invasi-lebanon-di-mana-posisi-pasukan-perdamaian-pbb-unifil on 20 January 2025

Center for Strategic Studies. (2023). Hezbollah and Cyber Warfare: Analyzing Communication Infrastructure Attacks. Washington, D.C.: CSS. https://www.csis.org/analysis/understanding-hamass-and-hezbollahs-uses-information-technology on January 20, 2025

C. Sheng et al., "Pager Explosion: Cybersecurity Insights and Afterthoughts," in IEEE/CAA Journal of Automatica Sinica, vol.

11, no. 12, pp. 2359–2362, December 2024, doi: 10.1109/JAS.2024.125034.

Daher, A. (2024). Militant Islamism in Lebanon and the War on Gaza. Mediterranean Politics, 1–10. https://doi.org/10.1080/13629395.2024.2439685

Estriani, H. N., Dewanto, P. A., & Asyidiqi, H. (2023). Asymmetric and Hybrid Warfare in Postmodern Times: Lesson from Hezbollah-Israeli War 2006. Andalas Journal of International Studies (AJIS), 12(1), 27-37.

Haaretz. (2024). "How Israel's Bulky Pager Fooled Hezbollah." Accessed via https://www.haaretz.com/israel-news/2024-10-17/ty-article-magazine/how-israels-bulky-pager-fooled-hezbollah/00000192-965c-d5a0-afbe-967f84680000

Haas, E. (1953). The Balance of Power: Prescription, Concept, or Propaganda? World Politics, 5, 442–477. https://doi.org/10.2307/2009179

Hendrianto, E. L. (2021). Israel's Cybersecurity Strategy in Dealing with Cyber Threats to Maintain National Security Stability. LINO Journal of International Relations, 1(2), 137-146. https://doi.org/10.31605/lino.v1i2.1157

Hoffman, F. G. (2007). Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies.

Jönsson, C. (2022). Theorising diplomacy. The Routledge Handbook of Diplomacy and Statecraft, 13–26.

Kaldor, M. (2013). New and old wars: Organised violence in a global era. John Wiley & Sons

Kahn, M. (2021). Hybrid Warfare and the Future of Conflict: The Case of Hezbollah. London: Palgrave Macmillan

Khatib, L. (2025). Hezbollah's state capture in Lebanon. Small Wars & Insurgencies, 1–22. https://doi.org/10.1080/09592318.2025.2477338

Khayyat, Y. (2025). When the southerners return. Human Organization, 1–5. https://doi.org/10.1080/00187259.2025.2451838

Libicki, M. C. (2009). Cyberdeterrence and Cyberwar. RAND Corporation.

Lynch, M. (2018). The new Arab order: power and violence in today's Middle East. Foreign Aff., 97, 116.

Magramo, Kathleen., Tanno, Sophie., Radford, Antoinette., Chowdhury, Maureen., Sangal, Aditi., Powell, Tori B., and Magramo, Kathleen. (2024) "Walkie-talkies explode in Lebanon the day after deadly pager attack." Accessed via https://edition.cnn.com/world/live-news/lebanon-pagers-explode-hezbollah-israel-09-18-24-intl-hnk/index.html

Mearsheimer, J. J. (2001). The tragedy of great power politics. W. W. Norton & Company.

Moore, M. (2024). "Reporter's Notebook: A walkie-talkie exploded at a funeral in Lebanon. Chaos ensued.". Accessed via https://abcnews.go.com/International/reporters-notebook-walkie-talkie-exploded-funeral-lebanon-chaos/story?id=113818269

Morgenthau, H. J. (1968). Organization of a Power System: Unilateralism and The Balance of Power. Naval War College Review, 20(7), 3-11.

Muhammad, A. (2023). The Geopolitical Implications of Shifting Alliances in a Multipolar World. Ulusal ve Uluslararası Sosyoloji ve Ekonomi Dergisi, 5(2), 410-430.

Nadirah, S. P., Pramana, A. D. R., & Zari, N. (2022). Qualitative, quantitative, mixed method research methodology (managing research with Mendeley and Nvivo). CV. Azka Pustaka.

Nye, J. S. (2010). Cyber power. Harvard University Press.

Odgaard, L. (2007). The balance of power in Asia-Pacific security: US-China policies on regional order. Routledge.

Defense, K. (2015). Indonesia's defense white paper. Jakarta: Ministry of Defense of the Republic of Indonesia.

Reichborn-Kjennerud, E., & Cullen, P. (2022). What is hybrid warfare? Norwegian Institute for International Affairs (NUPI).

Salim, A. R. M. (2016). Scenarios of Strategic balance and instability in the Middle East. International Journal of Humanities & Social Science Studies, 56-76.

Sarjito, A. (2024). The Role of Intelligence Through Formulating State Defense Policy in Hybrid War. PRIEST: Interdisciplinary Journal of Public Affairs, 7(1), 74–88.

Sarker, P.P., Das, U., Varshney, N., Shi, S., Kulkarni, A., Farahmandi, F., & Tehranipoor, M.M. (2025). When Everyday Devices Become Weapons: A Closer Look at the Pager and Walkie-talkie Attacks. ArXiv, abs/2501.17405.

Selján, P. (2024). The 7 October Hamas Attack. Academic and Applied Research in Military and Public Management Science. https://doi.org/10.32565/aarms.2024.1.5.

Solmaz, T. (2022). Hybrid warfare': One term, many meanings. Small Wars Journal, 25.

Smith, J. (2020). Cyber Warfare and Hybrid Conflicts: The New Age of Military Strategy. New York: Routledge

Stahl, L., Aliza, C., Shachar B., Jinsol J. (2024). "Israel's spy agency, Mossad, spent years orchestrating Hezbollah walkie-talkie, pager plots." Accessed via https://www.cbsnews.com/news/israeli-mossad-pager-walkie-talkie-hezbollah-plot-60-minutes/ on January 18, 2025

CNN (2024). "Why did Hezbollah's walkie talkie explode?". Accessed via https://www.cnnindonesia.com/teknologi/20240919111532-185-1145956/kenapa-walkie-talkie-hizbullah-bisa-meledak

Tobin, B. (2024). "Legality of cyber operations in the Israel-Hezbollah war". Centre for International Law. Accessed via https://cil.nus.edu.sg/blogs/legality-of-cyber-operations-in-the-israel-hezbollah-war/

Tuck, C. (2017). "Hybrid War: The Perfect Enemy". Accessed via https://defenceindepth.co/2017/04/25/hybrid-war-the-perfect-enemy/ on January 31, 2025

Walsham, G. (2006). Doing interpretive research. European journal of information systems, 15(3), 320–330.

Waltz, K. (1979). Theory of international politics. McGraw-Hill.

Widyoseno, B. (2024). THE EFFECTIVENESS OF THE ROLE OF THE UNITED NATIONS INTERM FORCE IN LEBANON IN RESOLVING THE ISRAEL-HEZBOLLAH CONFLICT IN 2023. Diplomacy and Global Security Journal: Journal of Master's Students in International Relations, 1(1).

Woodward, M. (2024). "Pager and walkie-talkie attacks on Hezbollah were audacious and carefully planned." Accessed via https://www.theguardian.com/world/2024/sep/18/pager-and-walkie-talkie-attacks-on-hezbollah-were-audacious-and-carefully-planned

Yulianto, M. A. (2013). LEBANON – PRE AND POST-WAR 34 DAYS ISRAEL VS HEZBOLLAH. Gramedia Pustaka Utama.

ABOUT THE AUTHORS

Regina Rivera, email: regina.44322002@mahasiswa.unikom.ac.id

Regina Rivera Rafa Dany is an international relations academician pursuing a bachelor's degree at Universitas Komputer Indonesia. Her compassion for humanity makes war and peace a compelling topic to explore. She hopes that she can contribute to a better and more equal world through all her work.

M Rivaldi Naufal is an Muhammad Rivaldi Naufal Buldansyah is an International Relations student at Universitas Komputer Indonesia. As an aspiring global thinker, he envisions a peaceful world where dialogue and diplomacy prevail. He believes international cooperation, understanding diverse cultures, and addressing global inequalities are key to achieving lasting peace. Rivaldi hopes for a future where nations work together.

N Merlin Cahyawati is an international relations student at Universitas Komputer Indonesia who critically thinks about the many conflicts in all countries. Merlin believes that in the future, all countries can create cooperation with full justice and peace. With the education he is pursuing, he hopes to influence how countries can collaborate peacefully, wisely, and prosperously.

Muhammad Farhan Rasyidi is an International Relations student at Universitas Komputer Indonesia. With a critical eye and a solutions-oriented mindset, Farhan navigates the complexities of international relations. They firmly believe that innovative collaboration and a commitment to ethical leadership can address even the most entrenched global challenges. Their work reflects a deep-seated hope for a future where diplomacy triumphs and shared prosperity becomes a reality.

Dewi Triwahyuni has been the head of the Department of International Relations at the IndonesianComputer University since 2018. She began her career as a lecturer in 2005. Dr. Triwahyuni holds a Bachelor's, Master's, and Doctoral degree in International Relations. As a professional lecturer and a Certified International Qualitative Researcher (CIQaR), she actively researches and writes scientific papers focusing on International Relations, U.S. Foreign Policy, and Cybersecurity.