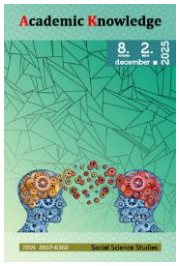
Academic Knowledge 8 (2),



Makalenin Türü / Article Type : Araştırma Makalesi / Research Article
Geliş Tarihi / Date Received : 08.05.2025
Kabul Tarihi / Date Accepted : 12.09.2025
Yayın Tarihi / Date Published : 31.12.2025
Yayın Sezonu / Pub Date Season : Güz / Fall

Pagers Explosions in Lebanon: Electronic Warfare or Kinetic Warfare?

Gül Seda ACET İNCE*

Keywords:
Lebanon,
Electronic Warfare,
Kinetic Warfare,
Pager

ABSTRACT

This study examines the utilization of pagers to be explosive systems in Lebanon and analyzes the role of such devices as a part of electronic and kinetic warfare. The objective of the research is to discuss the altering and transforming dimensions of these methods from the perspectives of strategy, technology, and war. In this context, a theoretical infrastructure was created throughout the study with a conceptual-descriptive method, and for this purpose, first-hand sources such as crime scene analyses and second-group sources such as academic literature and media news were used. The thematic analysis method was employed in order to assess the operational and regional extents of the explosives detonated via pagers in the research. The findings acknowledge the usage of pagers in such detonations, revealing a hybrid war strategy in which electronic manipulation and physical placement are used together. This is to say, the method reflects proximity to electronic warfare besides kinetic warfare. Using pager-detonated explosives is an instance of the changing nature of modern warfare, challenging traditional distinctions between electronic and kinetic methods. In this regard, the said incidents have been involved in the literature as the most present instances of electronic warfare. Comprehending these tactics has great significance in terms of improving effective countermeasures against emerging threats and updating the present legal frameworks.

Lübnan'da Çağrı Cihazı Patlamaları: Elektronik Harp mi? Kinetik Savaş mı?

Anahtar Kelimeler:
Lübnan,
Elektronik Savaş,
Kinetik Savaş,
Çağrı cihazı

ÖZ

Bu çalışma, Lübnan'da çağrı cihazlarının patlayıcı sistemler olarak kullanımını incelemekte ve bu cihazların elektronik ve kinetik savaş bağlamındaki rolünü analiz etmektedir. Araştırma, bu yöntemlerin strateji, teknoloji ve savaş perspektifinden değişen ve dönüşen boyutlarını ele almayı hedeflemektedir. Bu kapsamda, çalışma genelinde kavramsal-betimleyici bir yöntem ile; teorik bir altyapı oluşturulmuş ve bunun için de olay yeri analizleri gibi birinci ağızdan kaynaklar ve akademik literatür ve medya haberleri gibi ikinci grup kaynaklar kullanılmıştır. Çalışmada, çağrı cihazıyla patlatılan patlayıcıların operasyonel ve bölgesel boyutlarının değerlendirilmesi amacıyla tematik analiz yöntemi kullanılmıştır. Elde edilen bulgular, bu tür patlatmalarda çağrı cihazlarının kullanımına işaret etmektedir. Bu durum, elektronik manipülasyon ile fiziksel yerleştirmenin bir arada kullanıldığı hibrit bir savaş stratejisini ortaya koymaktadır. Başka bir deyişle, söz konusu yöntem, kinetik savaşın yanı sıra elektronik savaşa olan yakınlığı da yansıtmaktadır. Çağrı cihazıyla patlatılan patlayıcıların kullanımı, elektronik ve kinetik yöntemler arasındaki geleneksel ayrımlara meydan okuyarak modern savaşın değişen doğasının bir örneğini teşkil etmektedir. Bu çerçevede, bahsi geçen olaylar elektronik savaşın en güncel örnekleri olarak literatürde yerini almıştır. Söz konusu taktiklerin anlaşılması; ortaya çıkan tehditlere karşı etkili karşı önlemlerin geliştirilmesi ve mevcut yasal çerçevelerin güncellenmesi açısından büyük önem taşımaktadır.

* Assist. Prof. Dr. Malatya Turgut Özal University, seda.acet@ozal.edu.tr, 0000-0003-3329-7480

Acet İnce, G. S. (2025). Pagers explosions in Lebanon: Electronic warfare or kinetic warfare, *Academic Knowledge, 8*(2), 115-126. https://doi.org/10.5281/zenodo.18070118

1. INTRODUCTION

Warfare and engagement methods have significantly transformed throughout history, influenced by technological developments and strategic needs. Traditional warfare tactics to modern electronic warfare (EW), the role of technology in altering dynamics on the battlefield has become increasingly evident. Utilizing communication devices and digital technologies in conflicts has redefined military tactics and the legal and ethical aspects of war. In this regard, usage of pagers in Lebanon symbolizes a critical point of discussion. The question of whether said events are subsumed in EW context or traditional kinetic warfare (KW) context emerges complex issues requiring a comprehensive examination by strategic perspective.

Employing electromagnetic waves to disable, mislead, or deflect enemy communication systems has turned EW into a critical component of recent military tactics. The regulation of communication devices to trigger explosives or disrupt enemy operations demonstrates a byzantine aspect of EW in this respect. Current sources on the subject emphasize the increasing significance of aforementioned technologies in modern conflicts (Sarker et al., 2025; Rid, 2012: 6). For instance, there is evidence that enhanced EW systems applied by countries, i.e. the United States and Israel, are useful tools to deactivate enemy communications networks and invalidate missile defense systems (Youvan, 2024: 5-7). These instances demonstrate the potential for seemingly ordinary means of communication, such as pagers, to play critical roles in military operations.

Events involving the detonation of explosives via pagers exhibit a unique challenge transcending the extent of traditional electromagnetic warfare in the Lebanese case, which may also involve kinetic elements such as the physical setting and ignition of explosives. Therefore, the transformation of radio devices into means of triggering explosions requires an examination including both electromagnetic and kinetic perspectives.

KW traditionally includes direct physical assaults and the placement of explosives in order to achieve military objectives. Academic discussions highlight that such operations often aim enemy infrastructure or personnel. Using pagers as explosive devices, however, expands the traditional definition of KW, seeking the integration of technological tools with physical operations. In conflict areas, like Lebanon, this combination of electronic and kinetic methods reveals substantial concerns about the compatibility of these innovations with military doctrines, national security strategies, and international legal standards.

The objective of the study is to examine the common use of pagers in Lebanon within the context of the dual perspectives of EW and KW. This study also intends to enlighten how such situations obscure the boundaries between the two conflict areas and reflect new orientations in modern military strategies. This analysis utilizing the existing literature, proposes insight into the theoretical and useful aspects of these states in Lebanon.

The key finding of these analyses is that the pagers detonations in Lebanon have been the primary considerable incident to understand the interaction between EW and KW, forming a new category of “electronic-kinetic hybrid warfare” by pointing that EW is no longer just a “complementary” yet a direct “killer strategy.” The Lebanese incident is a novel milestone in the conceptual map of modern conflict in this sense.

The originality of the research is based upon two fundamental components: Theoretically, it demonstrates the "electronic-kinetic hybrid" class by combining electronic and

kinetic elements. Empirically, it examines mass explosions in Lebanon for the first time in accordance with this conceptual innovation. Thusly, apart from from the existing instances in the literature, the study concentrates on a mass attack with low-cost devices, proposing an original perspective on the future of EW.

The theoretical frameworks and the first section of this study are based upon the intersection of EW theory and KW principles. EW notions, such as signal detection, electromagnetic interference, and remote detonation, have been employed to understand the technological and strategic aspects of communication device utilizitation. KW principles, on the other hand, focusing on the physical placement and triggering of explosives, have been incorporated to analyze the operational perspectives of these cases. This double framework presented a structured lens in order for examining the coincidence and differentiation between electronic and kinetic methods in recent clashes. Other sections of this research consist of technical analyses of explosions in Lebanon. Finally, it was concluded that these incidents could be remarked to be a new generation of EW.

2. METHODOLOGY

A descriptive and analytical approach was adopted in the analysis of pager detonations in Lebanon in present research. Both the electronic and physical aspects of hybrid warfare challenges to directly assess the phenomenon by experimental methods, and, hence, a qualitative-oriented analysis method was preferred. The descriptive dimension allows the historical and technical aspects of events to be documented, and the analytical dimension allows these data to be interpreted within the framework of war theories as well. Hence, it was aimed to elucidate not only the event itself, but also its place in the literature on EW and KW.

The data of the study are gathered in two steps. Primary sources are reports of conflicts, field investigations, and firsthand statements of events stated by the media. Secondary sources involve academic studies on EW and hybrid warfare, security reports, and expert remarks on hybrid warfare and cyber threats. The data obtained from the sources were reviewed via the thematic analysis technique. Information on various aspects of the situation was coded, and recurrent themes (e.g., interventions in the pagers' supply chain, remote detonation capability, hybrid war tactics, legal restrictions) were determined. Afterwards, these themes were associated with the theoretical framework of EW and KW. This approach allowed the aggregation of data from various sources and the systematic presentation of a new dimension of hybrid warfare.

In terms of validity and reliability, various sources (media news, academic research) and different types of data were evaluated together. Nonetheless, methodological limitations include the lack of direct data collected by field research, the possibility of biased information transfer, and the politically sensitive nature of the issue. However, these limitations were designated in line with the objective of the study, and the findings were interpreted and presented in this regard.

This methodological approach aims to comprehend the technical components of the event and contribute to the literature on the character of hybrid warfare. Hence, the methodology of the research suggests a practical model to elucidate modern types of conflict by revealing the relationship between EW and KW.

3. THEORETICAL FRAMEWORK: DIGITAL TACTICS AND PHYSICAL POWER, ELECTRONIC WARFARE AND KINETIC WARFARE

EW has significantly transformed with the influence of technological developments in the 21st century, which enhancing the efficiency and strategic impact of the EW, turning it into a crucial part of contemporary military activities. The implementation of these technologies improves tactical decision-making processes and provides secure communication within EW systems.

It might be useful to investigate the various EW definitions existing in the literature. The most general form of EW is the management of a wide range of military operations. From a more comprehensive perspective, EW can function as an electronic system and may be used to intercept threat forces by aiming their electronic elements and deployments, to destroy enemy systems or diminish their function, and to prevent friendly troops from being detected or neutralized by electronic threats ("Electromagnetic Spectrum (EMS)", Ucar, n. d.). EW refers to the scientific, technological, and military studies carried out to ensure that friendly groups benefit from EMS efficiently, to avoid enemies from benefiting from this spectrum, or to minimize its usage (Cartwright, 2024). EW represents a technology warfare to control the EMS or to manage the EMS in a way that they are not able to utilize it against others by assessing the technological opportunities in the most efficient way (Sfetcu, 2024: 3-4).

The information struggle in the cyber world is often referred to as "cyber war" or "cyber conflict"; however, in reality, it includes an EW component and is a type of warfare involving the implementation of information and communication technologies to reach strategic goals in the digital environment (Çelik, 2018). Different from traditional conflicts, the main target of the information struggle is the enemy's information systems, data, and communication infrastructures, and it aims to employ various methods to seize, disrupt, manipulate, or gain advantage over these systems.

The activities conducted within the scope of EW are as follows: (Yang et al., 2024). Electronic Support (ES), Electronic Assault (EA), and Electronic Protection (EP). Electronic Support, ES: It is the process of detecting, classifying, identifying, and locating electronic system broadcasts of friendly or enemy units. Electronic Assault, EA: It intends to intercept and damage or temporarily disable enemy systems utilizing electromagnetic energy. EA refers to the usage of electromagnetic energy, directed energy weapons, and guided missiles to neutralize or destroy the rival's personnel, systems, and facilities, and it can be explained by the use of electromagnetic energy, directed energy weapons, and guided missiles to neutralize or destroy opponent personnel, systems, and facilities. Electronic Protection, EP: It involves methods and strategies applied to protect the electronic systems of friendly forces from enemy menace. It is defined as EW, involving activities that ensure the effective (active or passive) usage of EMS, avoiding the impacts of friendly forces or defective interventions, regardless of the actions of the enemy (Holcomb, 2024: 2).

EW helps in the effectiveness of techniques, tactics, and processes and military activities by providing knowledge domination. Two precise factors are needed in order to achieve success in EW. The first is to obtain innovative technologies that have not yet been recognized by others and to be able to produce and employ systems with said novel solutions; the second is to perform an effective intelligence study (Grant and Collins, 1982).

Reviewing the historical development of EW, it is seen that it was first utilized to confuse radio messages during the Russo-Japanese War in 1905. Subsequently, it is seen that it was reemployed by states in many events, such as World War II, Cold War, Vietnam War, and Gulf War (Dudczyk and Kawalec, 2015: 395). With the proliferation of digital technology, constantly evolving cyber threats have taken a new form, and their effects on military operations and information security have been increasing (Çalışkan, 2023). EW is often utilized to spread misinformation, divide and direct the public to induce imbalance in political structures or damage institutional trust (Özdemir and Uluyol, 2021: 651).

Similar to traditional EW signal jamming methods, operating system attacks are generally used to render networks, web pages, or services exposed to intense internet traffic inaccessible. With the development of technology, the EW sector in the field of information security will continue to progress, and the enhancement in artificial intelligence, quantum computing, and internet of things devices will propose new opportunities and challenges for both attackers and defenders (Çam et al., 2019: 4). EW activities involve the inhibition of communications, data collection in the digital era, where information has become a valuable resource, and mapping the network structure of the target. In terms of information security, this approach may be utilized to specify defects in a target's defense systems and to enable the abuse of these defects (Özdemir and Uluyol, 2021: 653).

Thanks to technological advances, cyberspace and digital wars are consistently evolving, which makes it essential for organizations and governments to update their methods and technologies to protect confidential data and important infrastructure (Sertçelik, 2015). Along with the development of technology, the balance between attack and defense in the field of EW will remain very delicate, and this will bring up the necessity for permanent preparation and innovation in the field of information security (Korucu, 2021). Recent conflicts are increasingly described by the combination of traditional military operations with cyber and information wars, causing the emergence of a hybrid method of warfare and emphasizing the significance of EW.

Subsequent to EW, it is practical to review the KW resources. The placement of conventional weapons and explosives is conducted with the purpose of causing serious physical damage to the resources, assets, and powers of the opponents (Bird, 2020). KW, in contrast to cyber warfare, refers to the traditional form of warfare in which physical power and weapons are utilized (Wihl, 2015: 4). Conventional conflict includes the usage of physical or kinetic force to eliminate hostile components. KW refers to direct power effectiveness. This type of warfare has both kinetic and non-kinetic elements and promotes the probability of destruction by affecting not only the physical infrastructure but also the systems and networks a nation supports. KW constitutes a critical and persistent menace threatening national security, economic balance, and social welfare. The probable consequences of this case are not only instantaneous but also long-term (Veeneman, 2023).

KW actualizes the dynamics of classical military conflicts via bombs, tanks, and various weapons. Wars between countries involve conflicts with the enemy's army, navy, and other military units and forces occupying rival territories. The civilian population sometimes got involved in these clashes since they were trapped on the battlefield, joined militias or resistance groups, or since the war expanded to cover all kinds of purposes. Along with the

emergence of new methods of warfare that do not need a direct and obvious usage of force, the requirement for new words to refer to this situation has arisen. In this scope, the traditional way of fighting the army is named as "KW" (Chapple and Seidl, 2021: 5).

KW is the name of war types that still exist today, yet have undergone significant alterations due to a lack of technology (Lilienthal and Ahmad, 2015: 362). KW describes traditional military conflicts in which actual power is employed in such a way as to encompass components such as projectile weapons and explosives. This kind of warfare has been the main center of military tactics for centuries; however, it is increasingly enriched by non-physical methods that take advantage of cyber and information wars (Kott et al., 2015).

Recent advances in military technology have caused an increase in non-kinetic skills capable of inhibiting enemy battles without causing physical damage, including in areas such as cyber conflicts and information struggles (Smith, 2011: 670). KW is still quite essential in military operations, although its connotation is gradually decreasing in comparison of non-kinetic strategies, which means it is required to alter the way we consider and treat conflicts. In this sense, what is happening in Lebanon, KW or EW, or some other variety of warfare? will be discussed.

4. ANALYSIS OF PAGER EXPLOSIONS IN LEBANON FROM THE PERSPECTIVE OF ELECTRONIC WARFARE AND KINETIC WARFARE

The pager detonation in Lebanon on 17 September 2024 created a mass tragedy that led to severe injuries and casualties. As a result of these regular and simultaneous detonations, 42 people, 12 of whom were civilians, lost their lives; more than 2,800 individuals were injured in various ways (Helou, 2024: 1-2). The targeting of pagers in Lebanon shows how electronic devices might be abused in war and the need for further security measures against such attacks (Hejase and Hejase, 2015).

The event that occurred in Lebanon took place in history as a unique development, and brought with it a lot of questioning. Why have mobile phones been so common recently, and why has an old means of communication, such as a pager, still been utilized? Besides, what was the detonation method of the old pagers and who carried it out? How could aforementioned detonations have happened simultaneously? Was it an electric wave or a kinetic conflict? In this section, the answers to said questions will be tried to be revealed.

Depending on their structure and intended usage, the characteristics of pagers vary widely, simple communication devices to advanced intelligent systems. Recent pagers include numerous technologies that enhance functionality, such as wireless connectivity, user-friendly interfaces, and multimedia features. The pager, more commonly known as the "beeper", is a small and portable means of communication that can often receive digital or alphanumeric short messages via radio frequencies. These pagers, which were quite frequent in mobile phones for a while, were employed to transmit and receive waves. The first pager was patented in the United States in 1949 by inventor Alfred Gross. The word “pager” was officially registered by Motorola in 1959 (Yeh and Huank, 2013). In the 1990s, mobile phones started to substitute these tiny devices, and pagers were largely out of use.

Although the use of pagers is quite limited nowadays, it is a matter of curiosity why these devices are so popular in Lebanon in an environment where mobile phones are common. Hezbollah utilized pagers, which were no longer in use, to mislead Israel's intelligence

agencies, believing that Israeli leaders were being tracked by their mobile phones. In other words, Hezbollah selected pagers to overcome Israeli intelligence with claims of being monitored via mobile phones. Yet this situation has a background. The assassination of Fuad Shukur, the leader of Hezbollah, in the apartment where he was hiding in July 2024 is associated with the last phone call ("Who was Fuad Shukr?", 2024). It is stated that the call to be made to the seventh floor to facilitate the targeting between the surrounding buildings was probably performed by infiltrating Hezbollah's internal communication system ("WSJ: Phone Call Hezbollah", n. d.).

A similar situation happened in 1996 when Hamas leader Yahya Ayyash's Motorola Alpha mobile phone was handed to him to receive a call from his father through a collaborator who had arrived in Gaza. After the Israeli forces determined that the phone belonged to Ayyash, they detonated the 50-gram bomb placed on the phone (Ayhan, 2009: 105). Following these events, restrictions were imposed on the usage of mobile phones in Lebanon. As the risk of exposure to external interventions was lower, it was determined to prefer basic communication tools with simpler structure. Due to their conviction that Israel controlled the entire telecommunications network in the country, they tried to secure themselves in this way.

Following the occurrence of these assassinations, Secretary General Hassan Nasrallah instructed Hezbollah members in February 2024 to place their mobile phones in metal boxes (“Exploding pagers kill Hezbollah,” 2024), and mobile phones were replaced by pagers that work with analog systems. As the telephone exchanges were controlled by Hezbollah, it was believed that this would provide a high level of security. Nevertheless, Hezbollah did not have adequate modern tools, and it was decided to procure pagers with long battery life and high signal strength.

In line with aforementioned technical descriptions, the section will conclude with a discussion on whether the incidents in Lebanon qualified as KW or EW. The simultaneous explosions that occurred in Lebanon on 17 September 2024 severely influenced both the local and international community. What was the cause of these detonations? As is known, pagers receive signals from the network they are connected to, translate them into written form, and display them to their users. These devices have a simple working principle and the probability of being converted into weapons. The first probability is that these devices may explode due to overuse and heating. Nonetheless, the possibility of this is very low. This is because the phone devices utilized in Lebanon are AR 924 models produced by Taiwan-based Gold Apollo ("Apollo Wireless", n. d.), and these devices are equipped with lithium batteries. Lithium batteries do not have an explosion risk as a result of overheating; they only have combustion properties.

Moreover, the simultaneous occurrence of numerous explosions significantly diminishes the probability of other instruments heating together and exploding (Özer, 2024). Another option is to explode these instruments with remote signals. Nonetheless, taking into account the limited processing capabilities of pagers, it is seen that they do not have the hardware required for advanced remote blasting systems like smartphones. In other words, these devices do not contain complex circuit boards or microprocessors. Therefore, this is considered a weak possibility. The most widely admitted situation on a global scale is the intervention of the devices at the post-production supply chain stage and the placement of

explosives in them (O'Connell, 2018). Numerous international sources are reported to confirm this. The fact that pagers require radio frequency signals to perform their functions provides a substantial opportunity for the aim of detonation.

Experts state that these tools were tampered with after the production process and explosives were placed in them, and these explosions were made with codes determined remotely by the electricity obtained through the batteries in them (Fidan, 2024). In addition to the remote detonation of these devices, plans are also being made to establish a timed detonation interval or a remote triggering system coordinated with each other. Furthermore, aforementioned instruments have a proper design for integrating mini-explosives, facilitating the placement of explosives secretly inside devices (Bassam and Gebeily, 2024). Another noteworthy question here is how these devices were tampered with. One possible scenario is to intervene and add a minimum amount of explosives before the devices reach their final users during the production or supply phase (during transport). The fact that more than one explosion occurred in tandem supports this situation.

Consequently, pager explosions in Lebanon represents one aspect of EW. Israel's simultaneous detonation of these devices by placing bombs during the procurement phase is a demonstration of EW, a new dimension of warfare, taking its place in history as a significant development in intelligence, sabotage, and low-intensity conflict. As stated in the case study, EW utilizes directed energy to stop access to EMS, neutralize communication between technologies, and render this communication inoperable or destroy it, suggesting that it has a different meaning compared to KW and cyber warfare.

5. DISCUSSION AND CONCULISION

The difference between EW and KW has long been evaluated as a classic distinction within military strategy between “direct violence” and “modification of EMS,” however, this distinction is becoming gradually uncertain both theoretically and practically. However, the simultaneous explosion of thousands of pagers in Lebanon on 17-18 September 2024 and the explosion of pagers communication devices the next day have dramatically presented that electronic interventions may have direct kinetic effects (deaths and injuries). This situation invalidated the idea that EW was generally limited to the extent of its “non-lethal” actions, revealing that physical destruction could be caused through electromagnetic or hardware changes, hence questioning the analytical significance of conceptual separation (Bassam, 2024). Thus, detonations triggered by electronic devices should be put to a legal audit based upon the principles of discrimination and proportionality. In particular, the dual-use pattern of radios and pagers promotes the risk of expected civilian casualties. Hence, it is substantial to address the deadly consequences of EW not only from a military point of view, but also from the aspects of legitimacy, law, and ethics.

In the case of Lebanon, evidence that invisible triggers were planted in devices by infiltrating the supply chain indicates that EW is not only limited to spectrum dominance but can also have a strategic impact on hardware security and logistics processes. Therefore, the preservation of the differentiation between electronic and KW still offers a useful framework for operational planning, whereas the Lebanese situation reveals that this differentiation is becoming gradually indefinite in practice and has new normative issues in terms of supply

chain security, civil and military distinction, and proportionality principles ("Electromagnetic Spectrum Operations", 2023).

Even though the distinction between EW and KW continues to present an analytical framework in terms of operational planning, the Lebanese situation indicates that this distinction is becoming increasingly ambiguous. The fuzzing of the boundary between electronic intervention and kinetic outcomes leads to the emergence of new varieties in military tactics, raising concerns on supply chain security, and normative debates in the context of international law. Thusly, it has great importance that future research promotes novel classifications, interpreting the interaction of electronic and kinetic effects, and aligns them with legal supervision structures.

While the distinction between EW and KW still provides an analytical framework for operational planning, the Lebanese example demonstrates that this boundary is becoming increasingly blurred. The potential for kinetic consequences of electronic interventions has led to new forms of military tactics, concerns about supply chain security, and normative debates in international law. Therefore, it is important for future research to develop new classifications that interpret the interaction of electronic and kinetic effects and align them with regulatory control structures.

The study suggests that locations where explosives were detected using pagers are strategically important. Areas where incidents were concentrated, such as Sur and Baalbek, are known for their geopolitical locations and the presence of critical infrastructure and military targets. This suggests that the pager explosion was not a random act, but rather a deliberate act aimed at exploiting vulnerabilities in high-value targets. The lower prevalence of politically significant incidents in Beirut may suggest that conflict parties prefer to avoid locations where countermeasures would be more effective or where intervention is more likely.

From a technological perspective, the findings demonstrate the growing role of electronic devices in modern warfare. The use of pagers as explosives demonstrates the adaptability of simple technologies to complex military objectives and highlights the need for stronger regulatory and international cooperation mechanisms to combat the misuse of communications technologies. From a legal perspective, explosives triggered by pagers cannot be clearly classified within the framework of existing international law because they combine both electronic and kinetic elements. While EW typically involves non-lethal interference with communication and information systems, kinetic attacks involve direct physical destruction and damage. These hybrid methods combine both dimensions, blurring traditional legal distinctions and forcing a reassessment of legal norms applicable in modern conflicts. Therefore, updated and comprehensive regulations are needed in international law to control the use of new technologies and prevent abuses.

Ultimately, the study reveals the impact of pager-triggered explosives in Lebanon on domestic and international security and the dynamics of asymmetric warfare. Such hybrid tactics demonstrate how non-state actors are developing unconventional methods to balance their technological and strategic advantages against more powerful adversaries, revealing the changing nature of modern warfare. The findings highlight the importance of understanding these trends through an interdisciplinary analysis that brings together military strategy,

technology, and international law. As conflicts continue, policymakers, strategists, and legal experts must effectively manage these new methods and mitigate their humanitarian impact. This study also provides an important foundation for evaluating the consequences of hybrid warfare strategies and shaping future security plans.

REFERENCES

Apollo Wireless. https://www.gapollo.com.tw/discontinued-product/ Erişim Tarihi: 2.5.2025.

Ayhan, V. (2009). HAMAS: Filistin Direnişinde Politik İslam. *Ortadoğu Etütleri* 1(1), 99-134.

Bassam, L. & Gebeily, M. (2024). Israel Planted Explosives ın Hezbollah's Taiwan-Made Pagers, Say Sources. https://www.reuters.com/world/middle-east/israel-planted-explosives-hezbollahs-taiwan-made-pagers-say-sources-2024-09-18/(2024, 20 Eylül). Erişim Tarihi: 6.4.2025.

Bassam, L. (2024). Hezbollah Vows to Punish Israel After Pager Explosions Across Lebanon. https://www.reuters.com/world/middle-east/dozens-hezbollah-members-wounded-lebanon-when-pagers-exploded-sources-witnesses-2024-09-17/ Erişim Tarihi: 1.9.2025

Bird, D. A. (2020). *Real-Time and Retrospective Analyses of Cyber Security*. IGI Global.UK

Çalışkan, A. (2023). Siber Savaş: Bilgi Krizi mi Yoksa Güvenliği mi?. *Savunma ve Savaş Araştırmaları Dergisi*, 33(1), 1-32.

Çam, H., Aslay, F. & Özen, Ü. (2019). Yükseköğretim Kurumlarında Bilgi Güvenliği Farkındalık Düzeylerinin Ölçümlenmesi. *Yönetim Bilişim Sistemleri Dergisi*, 5(2), 1-11.

Cartwright, M. (2024). Allied Bombing of Germany. https://www.worldhistory.org/article/2430/allied-bombing-of-germany. Erişim Tarihi: 10.03.2025.

Çelik, S. (2018). Siber Uzay ve Siber Güvenliğe Mutlidisipliner Bir Yaklaşım. *Academic Review of Humanities and Social Sciences*, 1(2), 110-119.

Chapple, M. & Seidl, D.(2021). *Cyberwarfare: Information Operations in a Connected World,* Jones & Bartlett Learning.

Dudczyk, J.& Kawalec, A. (2015). Specific Emitter Identification Based on Graphical Representation of the Distribution of Radar Signal Parameters. *Bulletin of the Polish Academy of Sciences Technical Sciences*, 63(2), 391-396.

Electromagnetic Spectrum Operations. US. Air Force Doctrine Publication. 3-85. https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-85/AFDP%203-85%20Electromagnetic%20Spectrum%20Ops.pdf Erişim Tarihi: 1.9.2025

Exploding Pagers Kill Hezbollah Members and Others, Leave Thousands Wounded, Officials Say; Militant Group Blames Israel. (2024, 18 Eylül). Erişim adresi https://www.cbsnews.com/news/hezbollah-lebanon-explosions-pagers-israel-hamas-war/ Erişim Tarihi: 30.04.2025.

Fidan, H. (2024). Uzmanlar, Lübnan'daki Çağrı Cihazı ve Telsizlerin Patlamasına Üretim Sonrası Müdahalenin Neden Olduğunu Değerlendiriyor. https://www.aa.com.tr/tr/gundem/uzmanlar-lubnandaki-cagri-cihazi-ve-telsizlerin-patlamasina-uretim-sonrasi-mudahalenin-neden-oldugunu-degerlendiriyor/3334373#. Erişim Tarihi: 1.5.2025.

Grant, P. M. & Collins. J. H. (1982). Introduction to Electronic Warfare. *IEE Proceedings F (Communications, Radar and Signal Processing)* 129 (3),113–32. https://doi.org/10.1049/ip-f-1.1982.0020.

Hejase, A. J., Hejase H. J. & Hejase, J. (2015). Cyber Warfare Awareness in Lebanon: Exploratory Research. *International Journal of Cyber-Security and Digital Forensics* 4(4), 482-497.

Helou, M., Weinstein, E., Kalaji, J., Chaaban, T. & Yammine, K. (2024). Pager Explosion in Beirut: an Unprecedented Event. *Disaster Medicine and Public Health Preparedness* 18 (215), 1–2.

Holcomb, J. (2024). Methods to Reduce Electronic Warfare System Errors with Bit-Accurate Modeling and Simulation, *IEEE AUTOTESTCON, National Harbor*. 1-3, https://doi.org/10.1109/AUTOTESTCON47465.2024.10697507

Korucu, O. (2021). Yeni Normal Dünya Düzeninin Siber Güvenlik ve Bilgi Güvenliği Etkileri. *Yönetim Bilişim Sistemleri Dergisi*, 7(1), 44-60.

Kott, A., Buchler, N. & Schaefer, K. (2015). Kinetic and Cyber. *Cyber Defense and Situational Awareness*, 62, 29-45.

Lilienthal, G. & Ahmad, N. (2015). Cyber-Attack as Inevitable Kinetic War. *Computer Law & Security Review* (31), 390-400.

O'Connell, G. (2018, 13 Haziran). Army Technology. The future of Electronic Warfare in Europe. https://www.army-technology.com/features/future-electronic-warfare-europe/. Erişim Tarihi: 3.3.2025.

Özdemir, A. & Uluyol, Ç. (2012). Kamu Kurum ve Kuruluşlarında Bilgi Güvenliği Farkındalığı. *Türkiye Sosyal Araştırmalar Dergisi*, 25(3), 649-666.

Özer, E. (2024). Patlayıcılı Çağrı Cihazları Nerede Üretildi, Cihazlara Patlayıcı Nasıl Yerleştirildi?. https://t24.com.tr/yazarlar/eray-ozer/patlayicili-cagri-cihazlari-nerede-uretildi-cihazlara-patlayici-nasil-yerlestirildi,46420#google_vignette Erişim Tarihi: 28.04.2025

Rid, T. (2012). Cyber War Will Not Take Place. *The Journal of Strategic Studies,* 35(1), 5-32.

Sarker, P. P., Das, U., Varshney, N., Shi, S., Kulkarni, A., Farahmandi, F., & Tehranipoor, M. (2025). When Everyday Devices Become Weapons: A Closer Look at the Pager and Walkie-Talkie Attacks [Preprint]. Cornell University, Arxiv, https://doi.org/10.48550/arXiv.2501.17405

Sertçelik, A. (2015). Siber Olayler Ekseninde Siber Güvenliği Anlamak. *Medeniyet Araştırmaları Dergisi* 2(3), 25-42.

Sfetcu, N. (2024). *Electronic Warfare and Artificial Intelligence*. MultiMedia Publishing.

Smith, F. L. (2011). A Casualty of Kinetic Warfare: Military Research, Development, and Acquisition for Biodefense. *Security Studies*, 20(4), 663-696.

UCAR. Center for Science Education. Electromagnetic (EM) Spectrum. (t. y.). https://scied.ucar.edu/learning-zone/earth-system/electromagnetic-spectrum, Erişim Tarihi: 1.4.2025.

Veeneman, P. (2023). Digital Battlegrounds: Evolving Hybrid Kinetic Warfare. https://industrialcyber.co/analysis/digital-battlegrounds-evolving-hybrid-kinetic-warfare/ Erişim Tarihi: 10.04.2025.

Who was Fuad Shukr, the Hezbollah commander killed by Israel in Beirut?. (2024, 31 Temmuz). https://www.aljazeera.com/news/2024/7/31/who-isfuad-shukr. Erişim Tarihi: 20.04.2025.

Wihl, L. (2015). Training for the Combined Cyber / Kinetic Battlefield. *MODSIM World,* No. 9, 1-11.

WSJ: Telefon Görüşmesi Hizbullah Komutanı Fuad Şükür'ü Ölüme Götürdü. (t.y.). https://nupel.tv/wsj-telefon-gorusmesi-hizbullah-komutani-fuad-sukuru-olume-goturdu/, Erişim Tarihi: 15.04.2025

Yang, A., Chen, W., Luo, H., Si, H., Cha, J., Li, G., Shuoyan, W., Liu, R., Ru. Y., Yang & Z., hengxian. (2024). The Prospect of Electronic Warfare in the 21st Century: An Analysis of Electronic Warfare Equipment Innovation and Its Strategic Impact Based on the Fusion of Quantum Communication and Artificial Intelligence. *Applied Science and Innovative Research,* 8(4), https://doi.org/10.22158/asir.v8n4p196

Yeh, S. T. (2013). *Pager Havinga Call-Back Function*. Patent Application Publication.

Youvan, D. C. (2024). Emergent AI and Military Technologies: The Role of Israeli Defense Companies in Modern Warfare. [Preprint]. ResearchGate. https://doi.org/10.13140/RG.2.2.23432.84488