STRATEGIES XXI International Scientific Conference
The Complex and Dynamic Nature of the Security Environment,
Bucharest, Romania - February, 27th, 2025

DOI: 10.53477/3045-2309-25-17

PAGER EXPLOSIONS IN LEBANON – IMPACT ON REGIONAL AND INTERNATIONAL SECURITY

Lyubosvet STOEV, PhD,
Associate Professor, "Georgi Stoykov Rakovski"
National Defense College, Sofia, Bulgaria.
E-mail: l.stoev@rndc.bg

Zhivo PETROV, PhD,
Colonel, Associate Professor, "Georgi Stoykov Rakovski"
National Defense College, Sofia, Bulgaria.
E-mail: zh.petrov@rndc.bg

Abstract: *The article relates to the interlude of 2024 Israel-Hezbollah war, and focuses onto the cyberattack against pagers and other electronic devices in Lebanon and Syria on September 17 and 18, 2024. A brief chronology of events is presented, followed by a review of pager technology for one-way communication. Features of the explosive substance used were examined and a hypothesis was developed for the method of attack. Finally, the consequences of the attack are analyzed as the both sides marched towards a full-scale war.*

Keywords: *Israel–Hezbollah conflict; supply chain infiltration; supply chain security; international reactions; Electronic Warfare; Psychological Operations; Cybersecurity; Middle East conflict.*

Introduction

The 2024 conflict between Israel and Hezbollah in Lebanon marked a significant escalation in the long-standing tensions between the two entities, with far-reaching implications for the region and beyond. The war unfolded against the backdrop of persistent geopolitical rivalries, ideological divides, and a history of confrontations that have periodically erupted into violence.

The roots of the 2024 war can be traced to decades of unresolved disputes and hostility between Israel and Hezbollah, the Lebanese Shiite militant and political organization. Since its establishment in the 1980s, Hezbollah has positioned itself as a resistance force against Israeli actions in Lebanon and the broader region. Israel, in turn, has regarded Hezbollah as a major security threat due to its extensive arsenal of rockets and its close ties to Iran.

The immediate catalyst for the 2024 war was a series of border skirmishes in late 2023, which saw an increase in rocket fire from southern Lebanon into northern Israel. These attacks, attributed to Hezbollah, prompted Israeli retaliatory airstrikes. The situation was further inflamed by political developments in Lebanon, including economic instability and internal divisions, which Hezbollah exploited to consolidate its power. Meanwhile, Israel faced its own domestic challenges, including political polarization and debates over security policies, which shaped its response to the escalating tensions.

The war officially began in February 2024, following a large-scale rocket barrage launched by Hezbollah into northern Israel, targeting both military and civilian infrastructure. Israel responded with a massive aerial campaign aimed at degrading Hezbollah's capabilities, focusing on weapons depots, command centers, and launch sites embedded in civilian areas.

One of the defining features of the conflict was its intensity and scope. Hezbollah's arsenal, reportedly bolstered by advanced Iranian-made precision-guided munitions, allowed it to strike deep into Israeli territory, including major cities such as Haifa and Tel Aviv. This marked a significant escalation compared to previous conflicts, such as the 2006 war.

On the Israeli side, the Israel Defense Forces (IDF) employed advanced technologies, including artificial intelligence and drone swarms, to counter Hezbollah's tactics. Ground incursions into southern Lebanon were launched to dismantle tunnel networks and secure border areas. However, these operations faced stiff resistance from well-entrenched Hezbollah fighters, resulting in high casualties on both sides.

The war also saw significant civilian suffering. In Lebanon, Israeli airstrikes caused widespread destruction in Hezbollah-controlled areas, displacing tens of thousands of people. In Israel, rocket attacks forced millions into shelters and disrupted daily life. International humanitarian organizations reported a severe crisis in both countries, with urgent calls for ceasefires to address the plight of civilians. One of these events that caused mass civilian suffering was the exploding pagers attack, which unfold as follows.

1. Exploding Pagers Cyberattack

On September 17, 2024, hundreds of pagers were detonated in Beirut, in the Bekaa Valley, in the southern regions of Lebanon, as well as in the Syrian capital Damascus (where a Hezbollah delegation was located at that time). The first explosions started at 15:45 local time (UTC+3) and lasted for about an hour. The next day, digital radios, electric scooters, solar panels and laptops explode. More than 4,000 people were injured, and more than 30 were killed, including children. According to eyewitnesses, the pagers emitted an audible signal, which provoked the victims to bring the device to their face.

Initially, the media spread the notion that the pagers were infected with the virus, or were subjected to a DDOS attack that caused their batteries to overheat. Subsequently, it turned out that the explosions were due to an explosive substance - pentaerythritol tetranitrate (PETN).

1.1. Brief description of pagers

A pager, also known as a beeper is shown in Figure no. 1. It is a one-way communication device designed to receive short messages. Such messages are usually called alphanumeric for containing both digits and alphabet letters. A single radio relay station is capable of providing one-way text service coverage over a significant radius and to multiple users. Pagers are used by fire services, in emergency medicine, but also in logistics and in the restaurant and hotel business. The passive principle of one-way communication makes the pager a secure tool that does not reveal the location of its carrier and the fact of receiving the message.

Figure no. 1: A typical pager (Clipground.com)

The ill-fated pagers were supplied to Lebanon as part of a large order through frontmen and companies in a number of countries, while the pagers themselves were modeled after Gold Apollo Co., Ltd. is a Taiwanese manufacturer specializing in wireless paging systems. Founded in October

1995 by Hsu Ching-Kuang, the company initially produced numeric pagers for the domestic market. However, following the decline of pager services in Taiwan in 1999, Gold Apollo shifted its focus to international markets. By 2011, it had become a leading pager supplier, ranking first in the North American market and second in Europe.

In September 2024, Gold Apollo became embroiled in controversy when pagers bearing its trademark were linked to explosions in Lebanon targeting Hezbollah members. The company's founder, Hsu Ching-Kuang, denied involvement, stating that Gold Apollo had licensed its trademark to BAC Consulting, a Hungarian company responsible for the design and manufacturing of the implicated pagers. He stressed that the devices were not marked "Made in Taiwan" and that Gold Apollo played no role in their manufacture.

Gold Apollo's product line includes POCSAG/FLEX pagers and other short-range radio devices, such as restaurant paging systems. Despite the decline in pager usage due to the rise of smartphones, the company has maintained a presence in niche markets where pagers remain a reliable communication method.

The incident in Lebanon has led to investigations by Taiwanese authorities into Gold Apollo's business dealings and its relationship with BAC Consulting. The situation underscores the complexities of global manufacturing and brand licensing agreements.

1.2. Explosive substance - PETN

According to Sky News Arabia, the explosive substance used is penta-erythritol-tetranitrate PETN (or PENTA in Russian-language sources). In Figure no. 2 are shown Structural formula and powder of PENT. The explosive[6] was developed at the end of the 19th century in Germany and was used for military purposes during both world wars. High explosive with high detonation velocity (> 8000 m/s) and energy release (in pure form) about 1.5 times that of TNT (Childs, 1994). The substance is insoluble in water, but dissolves in some specific organic solvents, such as acetone and dimethylformamide. In turn, acetone is used in the production of lithium-polymer batteries. The electrolyte of the LiPo battery is a polymer gel in which lithium salts are dissolved.

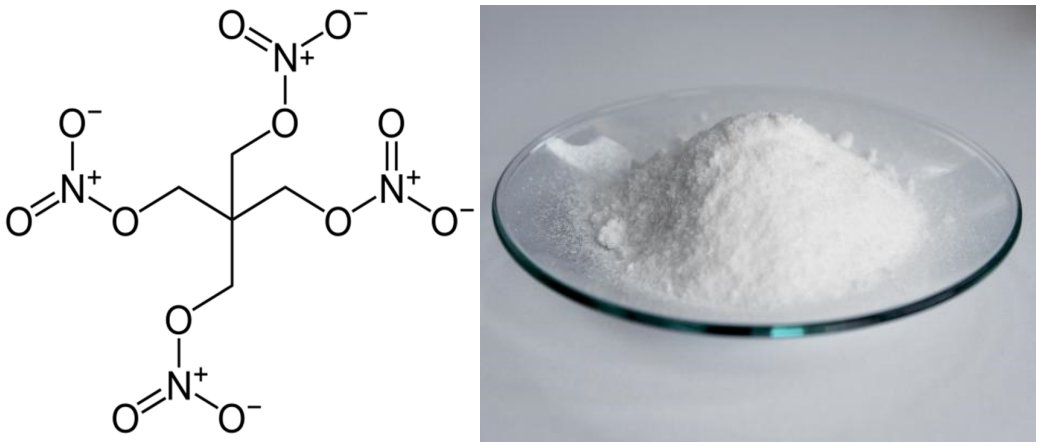

Figure no. 2: Structural formula and powder form of the explosive after laboratory synthesis (Wikimedia Commons)

In the case of exploding pagers (and subsequent radios, etc.), the world is witnessing the first exploding batteries. In figure 3 is shown internal structure of a lithium polymer cell, the author assumes that the explosive is dissolved in the electrolyte itself.

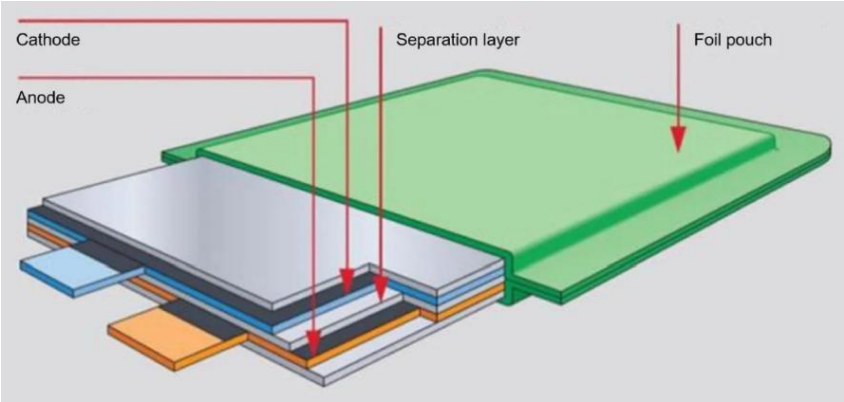

Figure no. 3: Internal structure of a lithium polymer cell.
(Mohammad Ghanaatpishe, 2014, "The lithium-ion battery modeling challenge:
A dynamic systems and control perspective")

1.3. Initiating the Explosions

According to eyewitness accounts, the blasts occurred an hour after 3:00 PM on September 17, 2024. They were preceded by a beep and a message prompting the victims to bring the device to their face. The media claim that the initiation takes place after a message is sent. However, this does not explain the large time interval in which the explosions occur. Expert assessment indicates that this is a cyberattack on the supply chain. This means that the malicious code that detonates the pagers is embedded as an alarm in the pager for the specific time (3:00 PM local time), the delay being either programmed or related to the accuracy of the clocks. The use of digital clocks allows a clockwork explosive to bet days, months and years ahead.

2. Consequences of the Explosions

The pager explosions on September 17, 2024, and the subsequent explosions of communications and other electronics the next day, had a large media coverage because of the many casualties, but, in practice, less than 0.3% of the victims of the attacks were linked to Hezbollah. Against this background, the escalation of the conflict on Israel's northern border continued with an increase in the intensity of airstrikes by the Israeli Air Force against Hezbollah targets in Lebanon and Syria. The ground operation of the Israeli army began with a long delay, and it was only talked about on October 1 of the same year. The significance of the September 17 and 18 blasts against the background of the airstrikes and the killing of Hezbollah's spiritual leader on September 27 is minimal.

Rather, the goal of the Israeli military and political leadership was to provoke a more serious conflict, broadly involving Hezbollah and the government of Syria. Exactly this happened two weeks later, when the larger war between Hezbollah and Israel started and Israeli troops invaded Lebanon.

The attack in Lebanon can be characterized as an act of terrorism, which violates Protocol 2 of the Geneva Convention, which prohibits the uncontrolled mining of everyday objects for civilian use. Unfortunately, this is an act that "opens Pandora's box" and may be implemented on a smaller or larger scale in the future, given the mass and universal use of "smart" electronics. Therefore, vigilance and careful evaluation of the process of acquisition, implementation and use of electronic devices is necessary.

As for the Lebanon itself, the 2024 war had profound regional implications. Iran, as Hezbollah's primary backer, played a crucial role by providing material and logistical support, further entrenching its influence in Lebanon. This drew condemnation from Israel's allies, particularly the United States, which provided military and diplomatic support to Israel during the conflict.

Other regional actors, including Saudi Arabia and the Gulf states, condemned Hezbollah's actions but were cautious about openly aligning with Israel due to domestic sensitivities. Meanwhile,

Syria's role as a conduit for Iranian weapons to Hezbollah became a focal point of Israeli airstrikes, raising concerns about a broader regional war.

The international community was deeply divided in its response to the war. Western nations generally supported Israel's right to self-defense but urged restraint to minimize civilian casualties. In contrast, many in the Global South criticized Israel's actions, viewing them as disproportionate and highlighting the humanitarian toll in Lebanon.

The United Nations later attempted to broker a ceasefire, but negotiations were hampered by mutual distrust and conflicting demands. A temporary truce was eventually reached in late April 2024, mediated by France and Qatar, but it left many underlying issues unresolved.

3. Aftermath and Consequences

The 2024 war had a devastating impact on Lebanon, exacerbating its already dire economic crisis and further weakening state institutions. Hezbollah emerged from the conflict battered but still intact, claiming a symbolic victory by surviving the Israeli onslaught. However, its reputation among some Lebanese communities suffered due to the immense destruction and loss of life.

In Israel, the war reignited debates about the country's security policies and the effectiveness of its deterrence strategy. While the IDF inflicted significant damage on Hezbollah, the group's ability to sustain its operations underscored the limitations of military solutions to such conflicts.

The war also highlighted broader geopolitical dynamics, including the deepening divide between Iran and its regional adversaries, as well as the shifting role of global powers in the Middle East. The conflict underscored the urgent need for comprehensive diplomatic efforts to address the root causes of instability in the region, including the Israeli-Palestinian conflict, the role of non-state actors, and the influence of external powers.

The full scope of the security consequences of the Lebanon pager attacks are hard to fully comprehend. First of all, it is a clear example of a so-called supply chain attack on a large scale and involving both hardware and software components. Up to now, the Cybersecurity establishment has dealt only with software supply chain attacks using network repositories. The Lebanon attack shows that such threat exists also in the domain of global trade with consumer and civilian electronics and also the trade with various smart devices with implications for the Internet-of-Things security. In this regard the trust among the Middle East onto both Taiwanese makers and European vendors of such electronics has severely deteriorated.

In order to cope with such multi-domain supply chain threats there are a few approaches to be adopted:

First of all, the end users should not rely onto the vendor certification and previous records. All new devices should be extensively and thoroughly analyzed and checked. It is not enough to them to be disassembled and visually inspected. All internal components of sample items should be inspected and subjected to destructive analysis – both chemical and functional. The electronics should be scanned, remodeled and analyzed. Finally, the device firmware should be copied, inspected and separately ran to check for all possible internal states and signals. If the software is scrambled and obfuscated, or anything else does not pass the security and safety, all the purchase should be rejected. A good policy would be to share all information for attempted smuggling of harmful device publicly, in the same time taking action against the possible perpetrator.

Second, the supply chain should be diversified not only with regards to the devices, but to the components of the system. Thus, the batteries should come from one provider, even better, the devices should work with batteries common on the market.

Third, the software should be created by independent developers, trusted and employed by the very purchasing organization. A good practice is the adoption of open source software and also open design of the purchased devices. As such the open source devices are tested by the public and all their deficiencies are dealt with. Any deviation from the standard would be easily detected.

All the above measures should prevent future attacks of such scale and scope.

Conclusion

The whole 2024 war between Israel and Hezbollah in Lebanon was a stark reminder of the fragility of peace in the Middle East and the complex interplay of local, regional, and international factors driving conflict. While the immediate fighting may have subsided, the deep-seated issues that fueled the war remain unresolved, posing significant challenges for the region's future stability and security. The lessons of this conflict underscore the importance of dialogue, restraint, and sustained efforts to address the underlying causes of violence and build a more peaceful and prosperous Middle East.

From the point of view of the Cybersecurity and the security of physical electronic devices the attack showed an example to potential attackers all over the world. Such an attack requires a number of resources and most of all consistent financial resources, but otherwise it is not by anyway limited to state actors. That is why there are needed security policies which will not only help to increase trust in the vendors of equipment, but will also conduct screening tests for offensive and harmful items. Such security policies along with sharing incident info among at least the stakeholders will reduce the risk of repeating such events to acceptable levels.

BIBLIORAPHY:

AGGARWAL, Mithil et al. 2024. "Who made the exploding pagers? A messy global trail emerges behind deadly Lebanon blasts.", NBC News, Hong Kong, September 18, 2024.
https://www.nbcnews.com/news/world/taiwan-firm-denies-making-pagers-used-lebanon-explosions-rcna171594

CHILDS, John.1994. "Explosives: A dictionary of military history and the art of war". ISBN 978-0-631-16848-5.

GRANTHAM-PHILIPS, Wyatte et al. 2024. "What to know about the two waves of deadly explosions that hit Lebanon and Syria", Associate Press, New York, September 19, 2024.
https://apnews.com/article/lebanon-israel-hezbollah-pager-explosion-e9493409a0648b846fdcadffdb02d71e

JEREMY BOB, Yonah and LAZNIK, Jakob. 2024. "Pager detonations wound thousands, majority Hezbollah members, in suspected cyberattack", Jerusalem Post, September 18, 2024.https://www.jpost.com/breaking-news/article-820536

KATZ, Yaakov and HENDEL, Yoaz (2012) "Israel vs. Iran: The Shadow War", ISBN 13 978-1597976688.

MARX, Willem. 2024. "Did exploding pagers attack on Hezbollah in Lebanon violate international law?", National Public Radio, Washington DC, September 20, 2024. https://www.npr.org/2024/09/20/g-s1-23812/lebanon-israel-exploding-pagers-hezbollah-international-law

OHCHR. 2024. Press release, UN Office of the High Commissioner on Human Rights, September 19, 2024. https://www.ohchr.org/en/press-releases/2024/09/exploding-pagers-and-radios-terrifying-violation-international-law-say-un

SALHANI, Justin. 2024. "Exploding pagers, psychological warfare: Israel's attack on Hezbollah". September 18, 2024. https://www.aljazeera.com/news/2024/9/18/chk_exploding-pagers-psychological-warfare-israels-attack-on-hezbollah

Science Madness. 2023. "Pentaerythritol tetranitrate". Science Madness, July 31 2023.
https://www.sciencemadness.org/smwiki/index.php/Pentaerythritol_tetranitrate

Sky News Arabia. 2024. "Sources uncover that Mossad is behind the pager attacks. What happened?", Sky News Arabia, Abu Dhabi, September 17, 2024 (in Arabic).
https://www.skynewsarabia.com/middle-east/1742443