JOURNAL OF CULTURAL ANALYSIS AND SOCIAL CHANGE

Journal of Cultural Analysis and Social Change,
2025, 10(2), 2287-2294
ISSN: 2589-1316

The Supply Chain Vulnerabilities of Weaponizing Daily Consumer Technologies Used In Middle-East Conflexts: A Case Study of Israel Pager And Walkie-Talkie Operation Attacks in Lebanon from Non-technical Prospective

Nourhan El-Bayaa [1*], Osman Gultekin [2]

[1] *Faculty of Economics and Administrative Sciences, Istanbul Aydin University Istanbul,* TÜRKIYE
[2] *Faculty of Economics and Administrative Sciences, Istanbul Aydin University Istanbul,* TÜRKIYE*; Email: nourhanelbayaa@aydin.edu.tr*

*__Corresponding Author:__ nourhanelbayaa@aydin.edu.tr

Citation: El-Bayaa, N. and Gultekin, O. (2025). The Supply Chain Vulnerabilities of Weaponizing Daily Consumer Technologies Used In Middle-East Conflexts: A Case Study of Israel Pager And Walkie-Talkie Operation Attacks in Lebanon from Non-technical Prospective, *Journal of Cultural Analysis and Social Change*, 10(2), 2287-2294. https://doi.org/10.64753/jcasc.v10i2.1925

Published: November 16, 2025

ABSTRACT

Supply chain attacks pose an increasing threat to communication device security, particularly in war zones with limited monitoring and wide attack surfaces. On September 17 and 18, 2024, thousands of civilian-used pagers and walkie-talkies detonated simultaneously, killing scores of users, wounding thousands more, and causing street chaos and dread. An undetermined number of these devices belonged to Hezbollah members in Lebanon. This strike established a new sort of distant warfare: the clandestine mass weaponization of seemingly harmless objects to achieve military goals. Pagers and walkie-talkies, among other battery-powered devices, have been widely utilized in both military and civilian situations. This article conducts an examination and broadens its scope to include the approaches and strategies used in the supply chain of such devices, as well as the supply chain vulnerabilities discovered.

Keywords: Supply Chain Vulnerabilities, Weaponizing Consumer Technologies, Hybrid Warfare, Pager Attacks, Israel, Lebanon

INTRODUCTION

Supply chain security is now a top priority in global cybersecurity efforts. As communication devices and IoT technologies become more integrated into daily activities, users face unprecedented risks due to their vulnerabilities. Conflict zones with limited monitoring facilities present unique problems for device integrity and minimum surveillance capabilities. These flaws allow attacks to employ electronics as weapons, resulting in significant physical and operational destruction. As an example of that, in September 2024, Israeli intelligence operatives weaponized civilian communication devices and pagers to target Hezbollah militants in Lebanon. Israeli operatives allegedly tampered with pagers and detonated them remotely, resulting in the deaths or injuries of important Hezbollah operatives. Israel has already conducted clandestine operations against Iranian-backed groups in the region, including Hezbollah (Gebeily et al., 2024).

More specifically, Hezbollah's 2024 attack targeted its communication network, which has relied on pagers as a low-tech alternative to using captured cell phones since the 1990s. Prior offensive operations that used telephonic gadgets against them served as the impetus for this dependence (Sky News, 2024). They believed that their operators would be protected by employing simpler, less traceable communication techniques. However, Israel's advanced intelligence operations to monitor and control the supply chain were not impervious to low-tech

remedies. The strategy severely damaged Hezbollah's leadership (Gebeily et al., 2024). The assault revealed the extent to which Israel's intelligence services had weaponized even something as basic as pagers for assassination (Seibt, 2024).

In order to trick Hezbollah into purchasing the altered pagers, Israeli spies reportedly compromised the operation by setting up phony websites and shops (Gebeily, Pearson, and Gauthier-Villars, 2024). The devices were made by the assailants using hidden explosives that were impossible for X-rays to detect (Gebeily et al., 2024). Significant Hezbollah casualties occurred in Lebanon when these pagers exploded simultaneously and were followed by a walkie-talkie attack (Gritten, 2024; Sabbagh et al., 2024). This operation ushers in a new era of warfare, one in which intelligence and technology play a significant role in military strategy and statecraft (Tlozek, 2024).

Using the Israeli Pager attacks in Lebanon as a case study, this study examines supply chain attacks on communication devices with an emphasis on their prevalence rates in war areas. In order to provide a more comprehensive knowledge of the vulnerabilities that make communication devices vulnerable to supply chain attacks, the study aims to break down non-technical overviews. Additionally, this paper is highlighting the three essential elements of Israel pager attack chain which are: users, devices, and the supply chain. Devices serve as the attack tools, users as the attack targets, and the supply chain as the setting in which the attack is organized and carried out.

LITERATURE REVIEW

Because of our increasing reliance on interconnected systems and attack surfaces, it is important to pay close attention to Internet of Things (IoT) and communication devices while studying supply chain attacks. Ross et al. (2015) recognized the significance of lowering supply chain vulnerabilities and created a thorough risk management framework for information systems utilized by Federal agencies. It was underlined that maintaining the integrity of important systems requires rigorous adherence to architectural and secure sourcing practices (Ross et al., 2015).

The study McGuire and Linton (2024) proved that hardware vulnerabilities are commonly used to launch complex attacks. The focus was on threat modeling and novel attack vectors, including malicious firmware installation. The study found parallels with the 2024 Lebanon incident, when manipulated hardware devices, namely Gold Apollo AR924 pagers, highlighted the critical need of addressing supply chain vulnerabilities (McGuire and Linton, 2024).

Butun et al. (2020) addressed IoT-specific vulnerabilities, particularly those in conflict zones. The lack of control and the availability of hostile players in these environments increase the hazards associated with IoT ecosystems. Several solutions were explored, including robust architectures and restorative techniques, to improve system integrity during bad conditions (Butun et al., 2020).

Lastly, an overview of software-oriented supply chain assaults that are noteworthy for their cascading impact on system security was given by Wang et al. (2021). The results clearly demonstrated how compromised software updates and altered firmware would create vulnerabilities across networked computers, making the task of consolidated defenses more difficult (Wang et al., 2021).

Table 1. Shows a Comparison of Major Supply Chain Attacks (Zita and Zita, 2025).

TABLE I: Comparison of Major Supply Chain Attacks

Attack	Target	Attack Method	Impact
Stuxnet (2010)	Nuclear centrifuges	Firmware manipulation via USB drives	Physical destruction
Supermicro Attack (2018)	Server motherboards	Hardware implants in the supply chain	Potential espionage
SolarWinds (2021)	IT infrastructure	Malware in software updates	Gov./enterprise access
2024 Lebanon Incident	Communication pagers	Physical tampering w/ explosives	Loss of life

Weaponising Consumer Technology

The nature of warfare in the Middle East has undergone significant transformation in recent years, with increasing reliance on hybrid warfare tactics. These tactics involve a strategic combination of conventional military force and irregular methods, such as cyber operations, information warfare, and exploitation of civilian infrastructure. As noted by scholars, hybrid warfare deliberately blurs the lines between war and peace by

integrating psychological operations, cyberattacks, and covert activities, all designed to destabilize adversaries while preserving plausible deniability (ETH Zurich, 2023; London School of Economics [LSE], 2025).

A striking case of such tactics was observed in the September 2024 attacks in Lebanon and Syria, during which thousands of pagers and walkie-talkies detonated in a coordinated fashion. These devices, commonly used by both civilians and Hezbollah operatives, were reportedly manipulated to contain explosive materials and remotely detonated. The incident resulted in significant casualties and the collapse of Hezbollah's communication infrastructure. Initial reports refrained from direct attribution, but subsequent investigations widely linked the operation to Israeli intelligence agencies (Lieber Institute, 2024; Wikipedia, 2024).

Detailed analysis suggests that Israeli operatives established a front company to infiltrate the supply chain by distributing pagers and walkie-talkies laced with PETN, a powerful explosive. These devices were reportedly triggered through encrypted remote messages, allowing operatives to initiate mass detonation without direct physical presence. The tactic demonstrated the potential for remote, deniable operations to achieve strategic goals by targeting non-military infrastructure critical to adversarial operations (Lieber Institute, 2024; Anadolu Agency, 2024).

This incident is situated within a broader trend in the Middle East, where both state and non-state actors are increasingly merging cyber and kinetic methods to secure asymmetric advantages. Tactics range from disabling communication networks to leveraging psychological and media warfare, exploiting dependencies on technology to disrupt and demoralize opponents (ETH Zurich, 2023; Geopolitical Monitor, 2025). These developments have made traditional military responses more difficult, particularly when actors operate within civilian-populated areas and rely on deniable methods, complicating both legal attribution and proportionality assessments.

One of the key enablers of these hybrid tactics is the vulnerability of global supply chains. As consumer technologies become more integrated into daily life, and as components are sourced from a vast web of global vendors, adversaries are increasingly able to embed malware or physical threats into commercial products. Attacks may be staged during manufacturing, packaging, or through third-party distributors. This method of infiltration allows state actors to circumvent traditional military defenses and strike indirectly at military and civilian targets alike (Avetta, 2025; CybelAngel, 2025; National Cyber Security Centre [NCSC], 2025).

Taxonomy of HYBRID WARFARE

The weaponization of commercial electronics reflects a major shift in warfare methodology, where consumer trust in benign technologies is exploited for violent ends. These methods allow attackers to strike from a distance with minimal visibility and plausible deniability, thus bypassing conventional rules of engagement. Scholars emphasize that such developments pose severe challenges to sovereignty, the existing normative frameworks governing warfare, and the ability of international law to adapt to technological advances (BlueVoyant, 2023; European Institute of Relations [EIR], 2021; Saferworld, 2023).

The September 2024 pager and walkie-talkie attacks have also sparked widespread international debate over the need for regulating dual-use technologies and securing supply chains. While the immediate impact was strategic—crippling Hezbollah's communications—the broader effect included public fear, disruption to civilian infrastructure, and humanitarian consequences. These outcomes have underscored the necessity for legal and policy reform, particularly in areas concerning the regulation of remote warfare technologies (Tech Policy, 2024; Avetta, 2025; CybelAngel, 2025).

Although academic literature has focused extensively on hybrid warfare in the European context, especially in Ukraine, the direct weaponization of consumer electronics in the Middle East remains understudied. This gap points to an urgent need for further interdisciplinary research that examines regulatory reforms, evolving legal norms, and the socio-political consequences for affected civilian populations.

Overview of Israel Pager and Walkie-Talkie Attacks in Lebanon

The altered gadgets not only caused physical damage and fatalities, but also disrupted secure communication lines, highlighting the deadly impact of hardware-based attacks. Pagers and walkie-talkies, with standardized components and predictable supply chains, were presumably designed for general use. This incident highlights the growing sophistication of hardware attacks and their use of global supply chain vulnerabilities.

Hezbollah obtained the pagers from a Taiwanese company, Gold Apollo, which was a key link in the attack's supply chain. Gold Apollo, established in 1995, specializes in pagers and related communication technology. Gold Apollo, a tiny company with around 40 workers, has a major presence in the pager market, especially in North America and Europe (Gebeily et al., 2024).

Its devices are frequently employed in various areas, including security and emergency services. Adversaries may target these gadgets due to their extensive usage and reliance on trusted brands. Gold Apollo has a licensing deal with Hungarian company BAC Consulting, which allowed for the introduction of modified devices. The attackers used this approach to conceal their involvement and enable the fabrication and spread of infected pagers.

Attackers militarized everyday communication gadgets by implanting explosives or triggering mechanisms, turning them into clandestine assassination tools (Murphy, 2024). Fig. 1. Below shows A brief overview of the pager and walkie-talkie attacks (Sarker et al., 2025).

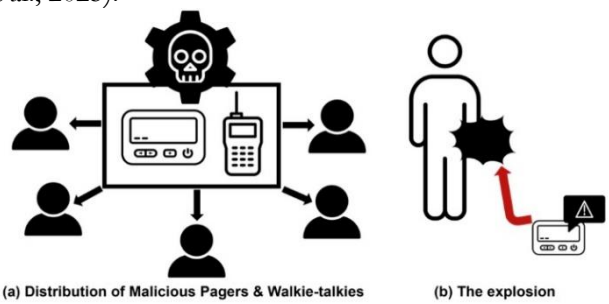

Fig. 1: A brief overview of the pager and walkie-talkie attacks

Investigations showed long-term preparations to supply modified pagers and walkie-talkies to Hezbollah-controlled areas (Sabbagh et al., 2024). The attacks are part of a covert operation with many entities from various nations. Several shell firms, including Norta Global and BAK Holding, distributed these devices under the cover of real trademarks such as Gold Apollo (Murphy, 2024). Financial activities between these businesses masked the provenance of the altered devices (Sabbagh et al., 2024). According to reports, these gadgets were introduced into Lebanon in 2015, around a year after their production was terminated. Figure 2 summarizes the timeline for walkie-talkie attacks. The timeline, which begins with the purchase of decommissioned ICOM walkie-talkies in 2014 and the creation of shell corporations in 2015, demonstrates a long-term monitoring and sabotage operation. Beginning in 2016, the modified devices entered Lebanon in 2023 and were finally ignited during the explosions on September 18, 2024. In terms of supply chain penetration and the technological adjustments made to the gadgets, the operation exhibits meticulous planning (Magramo et al., 2024).

In reaction to the war, the world community was sharply split. Western countries advised moderation to reduce civilian losses but generally supporting Israel's right to self-defense. On the other hand, a large number of people in the Global South denounced Israel's actions, pointing out the humanitarian cost in Lebanon and considering them to be out of proportion.

Later, the UN made an effort to mediate a truce, but negotiations were impeded by mistrust and divergent objectives. Through mediation by France and Qatar, a temporary truce was ultimately struck in late April 2024, but it did not address a number of fundamental problems. Fig. 2. explains the Timeline of planning and execution of the walkie-talkie attacks in Lebanon (Sarker et al., 2025).

Fig. 2: Timeline of planning and execution of the walkie-talkie attacks in Lebanon

Supply Chain Vulnerabilities

For supply chain management, PCBs which stands for printed circuit board, pose a special difficulty because they are sometimes the most technically demanding component of electronic assemblies and products. A specially designed PCB is needed for every assembly, in contrast to other, more common components. The three essential elements of Israel Pager attack chain are: users, devices, and the supply chain. Devices serve as the attack tools, users as the attack targets, and the supply chain as the setting in which the attack is organized and carried out.

The supply chain of cyberphysical devices, such as pagers, includes both hardware and software considerations. The hardware supply chain includes physical device manufacture, assembly, distribution, and logistics, while the software supply chain encompasses the creation, distribution, and deployment of software applications. An integrated supply chain of software and hardware components creates a broad ecosystem maintained by global providers, including networking equipment, devices, industrial systems, and applications. Prioritizing supply chain security is crucial as breaches can have serious implications, such as damage, disruption, or even complete destruction of operations (Yang and Peng, 2023).

Supply chain vulnerabilities, especially counterfeiting, pose a substantial risk to hardware security (Asadizanjani et al., 2017). Unauthorized or counterfeit PCBs, including cloned designs, damaged boards, and compromised materials, might enter the supply chain through unverified suppliers or intermediaries (Harrison et al., 2021).

The Taiwanese company, Gold Apollo, which was identified as the manufacturer of the infected gadgets, suffered serious harm to its reputation. Despite the lack of concrete proof connecting the corporation to deliberate

wrongdoing, its position in the worldwide supply chain made it the subject of intense scrutiny. Within weeks of the occurrence, Gold Apollo's stock worth reportedly fell by 15% as customers reassessed how dependent they were on its goods (Magramo et al., 2024). Taiwanese officials have interrogated people connected to Gold Apollo and searched many places. Additionally under examination and attention was the Hungarian business "BAC Consulting," which had a license to utilize Gold Apollo's brand (Murphy, 2024). To make matters more complicated, the incident also sparked questions over the involvement of other middlemen and shell corporations (Hale and McCready, 2024).

Because it brought attention to supply chain weaknesses and the possibility of technological abuse, the attack also had wider ramifications for the electronics and telecommunications sectors. Global need for supply chain audits and secure sourcing has increased for electronics and telecommunications companies. Taiwan's tech sector, which is essential to the world's electronics, has been under more scrutiny and pressure to guarantee the quality of its output (Mehta et al., 2022).

As companies were hesitant to purchase devices from vendors with inadequate traceability, manufacturers of similar devices—such as walkie-talkies, pagers, and other embedded communication systems—reported losses. These incidents acted as a wake-up call, drawing attention to the weaknesses present in international manufacturing networks and forcing other businesses to reconsider their procedures for quality control and procurement (Murphy, 2024).

In order to evade discovery, the delivery phase entails the surreptitious movement of armed devices to the target via standard supply chain channels. In order for attackers to forecast when and how the armed devices will reach the target, it is necessary to identify the source, destination, and path of devices in the supply chain during the reconnaissance phase. In more complicated situations, in order to precisely determine the attack's scope and possible damage, attackers might need to track the device's present position, owner, and surrounding people. Pagers and walkie-talkies' poor feedback capabilities caused collateral damage in the explosion incident, impacting both intended and unexpected targets (Murphy and Tidy, 2024).

The accomplishment of the attacker's goals, which could include tracking down employees, leaking data, or setting off explosions, constitutes the last phase of the cyber-physical attack chain. Even if the initial attack burst shows certain characteristics of the weaponized devices, it is still difficult to precisely identify which devices offer a real threat because the operation is typically carried out remotely. Widespread panic brought on by rumors or false alarms can occasionally cause greater disruption than the actual attack. Therefore, the best way to stop significant harm is usually to intercept the cyber-physical attack during the first three stages (Hale and McCready, 2024).

Given that the devices are probably armed at the production or distribution stages, the supply chain is regarded as the most vulnerable link, according to the incident study. The supply chain is unaffected, though, if there are no particular attack targets (users) or if the gadgets are not suited for weaponization. Therefore, as seen in Fig. 3, this is a security risk affecting not only the supply chain but the entire ecosystem of cyberphysical devices. Instead of focusing on a single area, we should improve the security of devices, the supply chain, and users as a whole to successfully stop future assaults (Sheng et al., 2024).

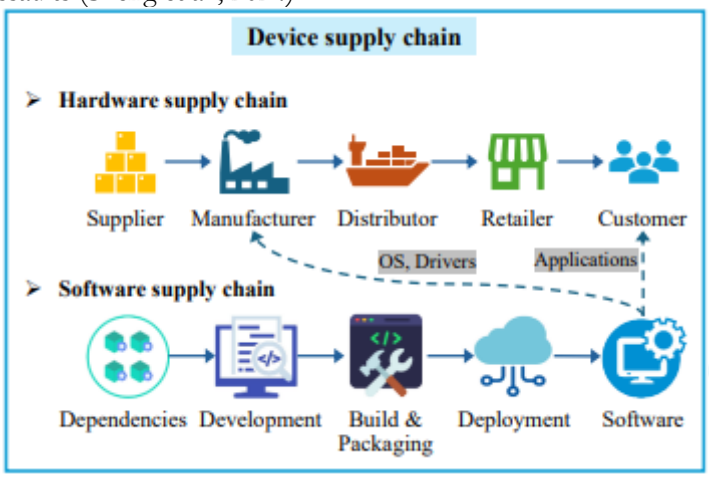

Figure 3. Device Supply Chain used in the Attack

Aftermath and Consequences

Following the pager and walkie-talkie attack, a number of theories on the attack and its execution surfaced from sources and experts. Lebanon suffered greatly as a result of the 2024 conflict, which made its already severe economic crisis worse and further weakened state institutions. Hezbollah declared a symbolic win by surviving the Israeli onslaught, emerging from the war bruised but unharmed. However, the massive damage and death toll

damaged its standing in several Lebanese communities. Debates concerning Israel's security policies and the efficacy of its deterrence strategy were rekindled during the war. Hezbollah was severely damaged by the IDF, yet the group's ability to continue operating demonstrated the limitations of using force to resolve such disputes (Hale and McCready, 2024).

The United States and other governments throughout the world kept a careful eye on the incident and its aftermath. Particularly in industries with vital communication systems, U.S. intelligence agencies voiced concerns about possible threats to their own supply chains (Feng, 2024). Calls for more funding for domestic manufacture and more security controls for hardware imports were sparked by the event, which raised concerns about foreign equipment used in sensitive activities. Additionally, Lebanon's government encountered difficulty in providing humanitarian help and securing its communication infrastructure. Regional governments in the Middle East reassessed equipment security, resulting in legislative changes and increased regulatory inspection of imported communication devices (Hale and McCready, 2024)

The consequences of failing to take preventive action to lower the risks posed by disrupted supply chains have been brought to light by the study. It is difficult to properly appreciate the extent of the security ramifications of the pager attacks in Lebanon. First of all, it is a blatant illustration of a large-scale supply chain attack that incorporates both software and hardware elements. Only software supply chain attacks utilizing network repositories have been addressed by the cybersecurity establishment thus far. The incident in Lebanon demonstrates that there is a threat to the security of the Internet of Things in the area of international trade in consumer and civilian electronics as well as trade in a variety of smart devices.

In this sense, the Middle East's confidence in Taiwanese manufacturers and European suppliers of these devices has drastically declined. The conflict also brought to light more general geopolitical factors, such as the growing gap between Iran and its neighbors and the changing role of superpowers in the Middle East. The Israeli-Palestinian conflict, the role of non-state players, and the influence of other powers are some of the primary reasons of instability in the region, and the war highlighted the urgent need for comprehensive diplomatic measures to address these issues.

RECOMMENDATIONS

To address supply chain vulnerabilities across several domains, consider the following approaches:

1. First and foremost, end users should not rely on vendor certifications and historical records. All new devices should undergo comprehensive and thorough analysis and testing. They require more than just a visual inspection after disassembling. All internal components of sample goods should undergo destructive investigation, including chemical and functional testing. Scan, modify, and analyze the electronics. To test for internal states and signals, copy and inspect the device firmware before running it separately. The entire transaction should be refused if the program is jumbled and obfuscated or if anything else fails security and safety checks. Publicly disclosing all information regarding attempted dangerous gadget smuggling while simultaneously pursuing legal action against the potential offender would be a smart approach.
2. Second, the supply chain ought to be diverse in terms of both the devices and the system's constituent parts. Therefore, the batteries ought to be supplied by a single supplier; better yet, the devices ought to be compatible with widely available batteries.
3. Third, the software should be developed by independent contractors who are engaged by the company making the purchase. Adopting open source software and making the products you buy openly designed are both smart practices. As a result, the public tests the open source devices and fixes any issues they have. Any departure from the norm would be readily apparent.

All of the aforementioned precautions ought to stop similar assaults in the future.

CONCLUSION

The entire 2024 battle between Israel and Hezbollah in Lebanon served as a sobering reminder of how precarious Middle East stability is and how intricately local, regional, and global elements interact to fuel warfare. Even if the direct fighting may have stopped, the underlying problems that led to the conflict have not been addressed, which presents serious obstacles to the peace and security of the area going forward. The lessons learned from this crisis highlight the value of communication, moderation, and persistent work to address the root causes of violence and create a more affluent and peaceful Middle East. The security issues pertaining to the battery supply chain have grown more serious, calling for careful analysis and preventative actions. We have illustrated the vulnerabilities of these devices by examining the cutting-edge attack vectors seen in the incidents headquartered

in Lebanon. We investigated workable solutions to supply chain assurance issues in addition to identifying the growing attack surfaces.

This viewpoint examines the attack from a non-technological standpoint, resulting in the explosion. The quick explosion of basic cyber-physical devices raises security problems for the sector. Our research highlights three key weaknesses in the Israel attack chain: people (users), devices, and the supply chain. To secure the cyber-physical device ecosystem, it's important to improve device, supply chain, and user security simultaneously. Attackers can exploit security flaws in these components, resulting in unexpected and perhaps dangerous attacks.

This attack set an example for potential attackers all across the world. This type of attack needs a significant amount of resources, particularly constant financial resources, and is not confined to state actors. Security measures should be implemented to build trust in equipment providers and screen for offending or hazardous things. Implementing security policies and sharing incident information with stakeholders can lessen the likelihood of similar situations occurring.

REFERENCES

Anadolu Agency. (2024, December). Israel planned pager attacks in Lebanon, Syria decade ago. https://www.aa.com.tr/en/middle-east/israel-planned-pager-attacks-in-lebanon-syria-decade-ago-say-former-mossad-officers/3432353

Avetta. (2025). Supply chain cyber risks: New frontiers in hybrid warfare. https://www.avetta.com

BlueVoyant. (2023). Weaponizing trust: Cyber vulnerabilities in consumer electronics. https://www.bluevoyant.com

CybelAngel. (2025). Supply chain attacks and the hybrid warfare threat. https://www.cybelangel.com

D. Mehta, J. True, O. P. Dizon-Paradis, N. Jessurun, D. L. Woodard, N. Asadizanjani, and M. Tehranipoor, "Fics pcb x-ray: A dataset for automated printed circuit board inter-layers inspection," Cryptology ePrint Archive, 2022.

EIR. (2021, February). Intelligence sharing in remote warfare. European Institute of Relations. https://www.eir.info

Emily Feng, (2024) "Tracking the exploding pagers used inapparent Israeli attack on Hezbollah," https://www.ualrpublicradio.org/npr-news/2024-09-18/tracking-the-exploding-pagers-used-in-apparent-israeli-attack-on-hezbollah, [Online].

Erin Hale and Alastair McCready, (2024) "Taiwan drawn into Middle East politics after deadly pager blasts in Lebanon," https://www.aljazeera.com/economy/2024/9/18/taiwan-dragged-into-middle-east-politics-after-deadly-pager-blasts, [Online].

Erin Hale and Alastair McCready, "Taiwan drawn into Middle East politics after deadly pager blasts in Lebanon," https://www.aljazeera.com/economy/2024/9/18/taiwan-dragged-into-middle-east-politics-after-deadly-pager-blasts, [Online].

ETH Zurich. (2023). Cybersecurity in the context of hybrid warfare. https://ethz.ch/en.html

Gebeily, M., Pearson, J. and Gauthier-Villars, D. (2024) How Israel's bulky pager fooled Hezbollah, 14 October, [Online], Available: https://www.reuters.com/graphics/ISRAELPALESTINIANS/HEZBOLLAH-PAGERS/mopawkkwjpa/ [25 October 2024].

Geopolitical Monitor. (2025). Hybrid warfare and asymmetric strategies in the Middle East. https://www.geopoliticalmonitor.com

Gritten, D. (2024) Death toll from Hezbollah pager explosions in Lebanon rises to 12, 18 September, [Online], Available: https://www.bbc.com/news/articles/cx2kn10xxldo [26 October 2024].

I. Butun, P. Osterberg, and H. Song, "Security of the Internet of Things: ¨ Vulnerabilities, Attacks, and Countermeasures," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 616–644, 2020.

J. Harrison, N. Asadizanjani, and M. Tehranipoor, "On malicious implants in pcbs throughout the supply chain," Integration, vol. 79, pp. 12–22, 2021.

J. McGuire and P. Linton, Hardware Supply Chain Security: Threat Modelling and Emerging Attacks. [Online]. Available: https://books.google.com/

J. T. Matt Murphy, "What we know about the hezbollah device explosions," https://www.bbc.com/news/articles/cz04m913m49o, online, September 20, 2024.

Kathleen Magramo, Antoinette Radford, Adrienne Vogt, Elise Hammond, Aditi Sangal, Matt Meyer,, "Lebanon rocked by deadly walkie-talkie and pager attacks," https://edition.cnn.com/world/live-news/lebanon-explosions-hezbollah-israel-09-19-24-intl-hnk/index.html, [Online, September 20, 2024].

Lieber Institute. (2024, October 11). "Well, it depends": The explosive pagers attack revisited. Lieber Institute for Law and Land Warfare. https://lieber.westpoint.edu/well-it-depends-explosive-pagers-attack-revisited/

LSE. (2025). Hybrid conflict and psychological operations in asymmetric war. London School of Economics and Political Science. https://www.lse.ac.uk

M. Murphy and J. Tidy, What we know about the hezbollah device explosions, 2024. [Online]. Available: https://www.bbc.com/news/ articles/cz04m913m49o (visited on 09/24/2024)

N. Asadizanjani, M. Tehranipoor, and D. Forte, "Pcb reverse engineering using nondestructive x-ray tomography and advanced image processing," IEEE Transactions on Components, Packaging and Manufacturing Technology, vol. 7, no. 2, pp. 292–299, 2017.

NCSC. (2025). Threats to national infrastructure through consumer supply chains. UK National Cyber Security Centre. https://www.ncsc.gov.uk

R. Ross, M. McEvilley, and J. Oren, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," NIST SP 800-161, U.S. Dept. of Commerce, 2015.

Sabbagh, D., Bayer, L. and Milmo, D. (2024) Pager and walkie-talkie attacks on Hezbollah were audacious and carefully planned, 2024 September, [Online], Available: https://www.theguardian.com/world/2024/sep/18/pager-and-walkie-talkie-attacks-onhezbollah-were-audacious-and-carefully-planned [26 October 2024].

Saferworld. (2023). Remote warfare and human security: Lessons from the Middle East. https://www.saferworld.org.uk

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. arXiv preprint arXiv:2501.17405.

Seibt, S. (2024) What the operation to blow up Hezbollah's pagers tells us about Israel's spy agencies, 20 September, [Online], Available: https://www.france24.com/en/middleeast/20240920-what-the-operation-to-blow-up-hezbollah-s-pagers-tells-us-about-israel-sspy-agencies-mossad-lebanon [25 October 2024].

Sheng, C., Ma, W., Han, Q. L., Zhou, W., Zhu, X., Wen, S., ... & Wang, F. Y. (2024). Pager explosion: Cybersecurity insights and afterthoughts. IEEE/CAA Journal of Automatica Sinica, 11(12), 2359-2362.

Sky News (2024) From exploding pagers to cyber warfare: Israel's long history of alleged secret operations, 2024 September, [Online], Available: https://news.sky.com/story/fromexploding-pagers-to-cyber-warfare-israels-long-history-of-alleged-secret-operations13217263 [25 October 2024].

Tech Policy. (2024, November). The weaponization of things: Israel's techno-violence. https://www.techpolicyreview.org

Wikipedia. (2024). 2024 Lebanon electronic device attacks. https://en.wikipedia.org/wiki/2024_Lebanon_electronic_device_attacks

Y. Wang, Y. Guo, and H. Wang, "A Survey of Software Supply Chain Attacks," ACM Computing Surveys, vol. 54, no. 5, pp. 1–36, 2021.

Y. Yang and C. Peng, "MPC-Based change management of supply chain under disruption risks: The case of battery industry.," IEEE/CAAJ. Autom. Sinica, vol. 10, no.9, pp.1896–1898, 2023.

Zita, N. (2025). Mitigating Supply Chain Risks in Communication Devices Across Conflict Zones. Authorea Preprints.

