

Lessons Learned from the Pager Attack: the Law of War, Warfighting, and the Weaponization of the Supply Chain

By Andrew Garbarino and Liam Bradley

January 6, 2025

On Sept. 17, 2024 and again on Sept. 18, 2024, Israel, through what has now been labeled a “supply chain interdiction” (SCI) attack, detonated previously intercepted pagers and other electronic devices used by Hezbollah and its affiliates. Hezbollah, an Iran-backed Lebanese militia that has been designated as a Foreign Terrorist Organization (FTO) by the U.S. government, was formed in 1982, describes itself as the “leader of Islamic resistance to Israel” and has conducted numerous attacks against Israel. See *Lebanese Hezbollah*, Congressional Research Service (Feb. 1, 2021), [Lebanese Hezbollah](https://www.congressionalresearch.org/lebanese-hezbollah) (justice.gov) (last visited Sept. 23, 2024).

In addition to acting as a heavily armed militia, Hezbollah acts as a regional player in the Middle East and exercises strong influence in Lebanon both as a political party and paramilitary organization. See *id.*

To effectuate the attack, Israeli agents are believed to have added small amounts of explosive material to a variety of devices, passed them along to Hezbollah agents during the 15 years preceding the attack and almost simultaneously detonated the devices in an attack that wounded 2,931 and killed 37. See Josh Margolin, *Israel had hand in manufacturing pagers that exploded in Lebanon: Source*, ABC



Andrew Garbarino and Liam Bradley

News (Sep. 19, 2024), <https://abcnews.go.com/International/israel-hand-manufacturing-pagers-exploded-lebanon-source/story?id=113851347>.

The stunning and unsettling impact of the SCI operation included 15 years of careful planning, during which Israeli intelligence officers fronted the compromised devices through a legitimate company to Hezbollah assets in Lebanon, has created legal, warfighting, and sourcing concerns.

SCI and the Law of War

The most prominent issue raised by the incident is whether the rules of war permit such an attack. It follows that the Law of Armed Conflict (“LOAC”) would be applicable to an operation of this kind.

LOAC is “a complex web of international treaties, customary laws, and domestic regulations that govern wartime conduct.” See “Law of Armed Conflict Beyond Black and White: Navigating the Gray Areas of Warfare,” Military Law Center, The Law of Armed Conflict: A Guide to Responsible Warfare (militarylawcenter.com).

Although all 196 of the world’s recognized nation states ratified the Geneva Conventions, the primary treaty underlying LOAC, uniformity has since deteriorated as subsequent protocols have not been uniformly ratified. See “Frequently asked Questions on the Rules of War,” ICRC (Jul. 20, 2023), Frequently asked questions on the rules of war | ICRC.

Although customary law should theoretically fill in gaps and serve to bind all states, there remains significant room for interpretation with regard to wartime conduct. See *id.* Depending on the treaties subscribed to by a given country, domestic regulations and its customary law, SCI attacks could be construed as permissible under LOAC.

With those principles in mind, five issues should be considered to evaluate any type of military action, including the SCI undertaken in Lebanon:

- **Military Necessity** – is the SCI operation permitted under LOAC and is the operation required to defeat the enemy?
- **Unnecessary Suffering** – will the SCI operation, or the manner in which it is carried out, cause unnecessary suffering?
- **Proportionality** – will the military advantage gained from the use of the SCI operation outweigh the anticipated collateral civilian losses?
- **Distinction** – can the SCI operation be employed in a manner that distinguishes between combatants and non-combatants or military targets from private property?
- **Honor** – would this type of operation be unfair or constitute a breach of trust with the enemy?”

See “Basic Principles of the Law of War and Their Targeting Implications,” LWI, Law of War Principles (institutelw.com)

The consideration of honor—not easily definable in any context—under LOAC is designed to encour-

age both adversaries to not take advantage of the other. This assessment is further complicated when fighting a non-state actor, which has not ratified any portion of LOAC.

While LOAC may permit SCI operations, whether or not a state may conduct a particular SCI operation will be highly dependent on the ability to assess those fundamental principles noted above.

SCI Got Results and May Reshape Warfighting

What SCI operations mean to the future of warfighting remains unclear. In a practical sense, the battlefield has become ubiquitous. What was a conflict between Hamas and Israel pivoted, over the course of only two days, and without a significant mobilization exercise, from Gaza to Southern Lebanon.

Additionally, the attack rendered Hezbollah without reliable communications, sowing distrust in devices and forcing face-to-face meetings of leadership. Israel took great advantage of this ensuing instability with airstrikes that targeted the leadership of both Hezbollah and the Iranian Revolutionary Guard Corps.

The result was something of a masterclass on three levels of warfighting: the tactical, operational, and strategic. Israel’s dramatic success in disabling communications through distrust, forcing high-value targets to meet face-to-face and then employing air power might prompt a reconsideration of the counterinsurgency operations (known as the “COIN doctrine”) used by the U.S. in both Iraq and Afghanistan.

A critical component to any successful military strategy is “winning the peace”: the civilian efforts following combat operations that provide for an exit strategy that rebuilds the community, fosters economic growth in the war-torn region and restores trust in responsive civilian institutions that will further undermine the recruitment/tolerance of terrorist activity. The outcome of these civilian efforts in Lebanon will ultimately determine the success of Israel’s overall strategy.

Pending the outcome of any civilian efforts, SCI operations may become a viable way to swiftly disrupt non-state actors by forcing them to cluster and behave as a more conventional force which the state actor

can leverage and exploit for rapid success on the now ubiquitous battlefield.

Industries and Governments Need to Revisit Supply Sourcing and Turn to “Friendshoring”

The supply chain may be a new battlefield as well. SCI operations will force critical industries and governments to revisit their sourcing for almost all supplies. The operation confirmed that technology that is used by nearly every American citizen might be weaponized in the future. Office phones, cell phones, routers and other electronics will require extra care in sourcing to ensure the components of the item can be traced to reliable and trustworthy suppliers throughout the supply chain.

The National Security Division of the U.S. Department of Justice has developed initiatives that focus on enforcing national security by holding business organizations responsible for violating export control and sanctions laws. It’s quite possible that more exacting and specific scrutiny of supply chain concerns will be next.

Suppliers, if they have not already anticipated the response, should be prepared to identify the precautions they have in place to prevent tampering and detail the entities from which they source materials. For those that needing to source materials overseas, the solution may be “friendshoring,” an emerging trade practice “where supply chain networks are focused on countries regarded as political and economic allies.” See Stefan Ellerbeck, *What’s the difference between ‘friendshoring’ and other global trade buzzwords?* World Economic Forum (Feb. 17, 2023), *What is ‘friendshoring’? This and other global trade buzzwords explained* | World Economic Forum (weforum.org).

Further implications might also include stricter workplace policies for use of personal devices around workplaces of critical industrial or govern-

ment offices to prevent “contamination” of securely sourced items.

In response to the SCI operation, Iran has already banned Motorola mobile phones due to security concerns. In the U.S., one must consider where cell phones and other electronics were manufactured (the authors are willing to bet that most of them are not made domestically.)

On a larger scale, the United States has been acutely aware of the threat posed by the significant number of Chinese components in U.S. electrical transformers throughout its power grid, but has yet to take action. The recent pager attack might be the catalyst for action. In that regard, government entities and critical industries should assess their exposure and, if necessary, adopt policies to defend against future SCI operations. Those in non-critical industries might be well-served to assess risks to their organizations as well.

With the world now on notice of modern day SCI operations and the devastating extent to which they can be used, militaries must evaluate LOAC on both the international and domestic level to determine what adjustments may be needed to applicable treaties and laws underpinning SCI operations.

Military leaders must find a way to ethically deploy SCI operations in light of the rapid success of Israel’s SCI operation against Hezbollah, while governments and the private industry must develop thorough policies and innovate new strategies to insulate themselves and defend against such SCI attacks. As the battlefield ever evolves and ever expands, SCI operations will undoubtedly have a major impact on the laws of war, warfighting, and global trade.

Andrew Garbarino is of counsel with *Ruskin Moscou Faltischek*, where he co-chairs the white collar practice group. **Liam Bradley**, an associate at the firm, is graduate of the *United States Military Academy*. **Sean Tierney**, an intern at the firm, contributed to the preparation of this article.