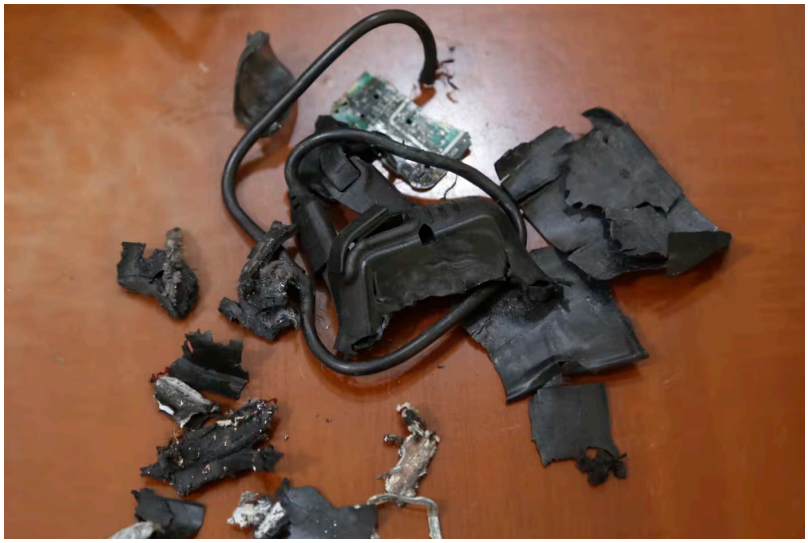
LOGISTICS REPORT

Pager Attacks in Lebanon 'Weaponize' Supply Chains

The path of thousands of exploding devices targeting Hezbollah remains murky, highlighting what experts say are risks in electronics supply chains

By Liz Young Follow

Sept. 20, 2024 3:02 pm ET



The remains of exploded pagers on display at an undisclosed location in Beirut's southern suburbs after the attack. PHOTO: AGENCE FRANCE-PRESSE/GETTY IMAGES

The attacks on Hezbollah this week using explosives planted inside electronics highlight the risks and vulnerabilities of technology supply chains, experts say.

"Every board, every CEO, government, has now woken up today to the fact that products that we buy could be compromised," said Bindiya Vakil, chief executive of supply-chain risk management firm Resilinc. "This is weaponizing of the supply chain."

The supply chain trail behind Israel's attack that began with exploding pagers remains murky, and the explosions of a range of electronics add to the questions around the origins of the devices that wreaked havoc across Lebanon, killing dozens and injuring thousands.

Many electronics manufacturers outsource production of relatively low-cost items such as pagers, which experts say makes it difficult to track and verify the source of each piece within the final product. Companies often ship their designs for devices off to contract manufacturers who handle sourcing the components and assembly of the final goods.

"There's multiple distributors, there's multiple contract manufacturers, there's multiple boards, there's multiple locations. It's just a really confusing array of people" in electronics supply chains, said Rob Handfield, a supply chain management professor at North Carolina State University.

Handfield said the complicated, multistep manufacturing process involving often far-flung suppliers introduces risk that parts inside finished products may be counterfeit or manipulated.

The added tiers in outsourced manufacturing make it harder for buyers to know where the goods and their components are coming from, said Jeff Williamson, head of sustainability at software firm Infyos.

"For companies in the sector, this is another example of how risky it can be to have limited oversight over particular supply chains and trade flows, as well as the business relationships underpinning certain companies," Williamson said.

Other vulnerabilities in commercial supply chains can be exposed after goods leave the factory, said Chris Clark, managing partner at supply chain consulting firm Todd Advisory and the former chief supply chain and procurement officer at Motorola Solutions.

When a shipment of finished goods arrives at a distribution center, "all of a sudden that control you had in the factory is no longer there," Clark said. Intruders "can swap out batteries, swap out components to put in whatever bad things they want to put in, and then it moves on," he said.

Shadowy networks

Supply lines for everything from food and medicines to military material are perpetually targeted in armed conflicts, but this week's attacks engineered by Israel mark an audacious effort to embed itself within Hezbollah's supply chain for communications equipment.

Investigations into how that happened so far point to a complicated, shadowy network of companies and individuals spanning from Asia to Eastern Europe to the Middle East.

Thousands of pagers carried by members of Lebanese militant group Hezbollah exploded on Tuesday. The next day, walkie-talkies used by the group blew up in homes, cars and in operatives' hands across Lebanon. The attacks left at least 37 dead and nearly 3,000 injured.

A man holds a walkie-talkie after he removed the battery during the funeral of people killed when paging devices exploded in a deadly wave across Lebanon the previous day. PHOTO: ANWAR AMRO/AGENCE FRANCE-PRESSE/GETTY IMAGES

Investigations into the massive attacks point to a supply-chain intrusion in which Israel inserted explosives into devices that Hezbollah distributed to its members.

The Journal reported Israel appears to have laced the batteries of the devices with explosives. Israel then hacked into the hub of the group's pager network to simultaneously send a message to thousands of users that triggered the blasts.

The pager devices were similar to those produced by Taiwan-based Gold Apollo. That company said it didn't make the pagers and that they were designed and

built by a company named BAC Consulting Kft, registered in Budapest.

BAC has a shadowy history, however, with little evidence available that it is manufacturing electronics. A Hungarian government spokesman wrote on social-media network X that the pagers had never been in Hungary and that BAC Consulting is a "trading intermediary, with no manufacturing or operational site in Hungary."

Japanese radio equipment maker Icom said it no longer makes the walkie-talkies that appear to have been used in the attack in Lebanon, nor the batteries needed to operate them. The company said in a statement on its website that it sold the walkie-talkies in overseas markets, including the Middle East, from 2004 to October 2014 but discontinued the model about 10 years ago.

Icom said the radios were missing "a hologram seal to distinguish counterfeit products." Because of that, "it is not possible to confirm whether the product shipped from our company," Icom said.

Western governments in recent years have investigated and cracked down on foreign-made equipment due to national security concerns about spying and cyberattacks.

A U.S. congressional investigation this month found Chinese cargo cranes used at seaports around the country had embedded technology that could allow Beijing to covertly gain access to the machines.

The investigation uncovered instances where cranes came with cellular modems installed without the knowledge of port authorities and done so beyond the scope of contracts with the China-based manufacturer of the cranes, ZPMC.

The congressional report said the technology could be used remotely to interfere with U.S. infrastructure.

Write to Liz Young at liz.young@wsj.com