CENJOWS

WEB ARTICLE
WA/37/25

THE NEW FACE OF CONFLICT: WEAPONISED SUPPLY CHAINS AND TROJAN HORSES

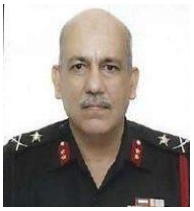
LT GEN (DR) SANJAY SETHI, AVSM, VSM

www.cenjows.in

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

The New Face of Conflict: Weaponised Supply Chains and Trojan Horses



Lt Gen (Dr) Sanjay Sethi, AVSM, VSM, currently serves as the Commandant of the Military College of Materials Management, Jabalpur & Chairman of the Sector Skill Council for Strategic Manufacturing (SSSDC) and the Colonel Commandant of AOC

Introduction

This article posits that the world has just passed the inflection point, where the *character of war* has been fundamentally altered. The factors contributing to this change include a combination of technology, open-source software, and the web of supply chains that fuel the economy.[i] A brief analysis of what the Israelis did in the pager attack on Hezbollah and, more recently, what the Ukrainians achieved in the drone attack would sufficiently vindicate the assertion. It would be interesting to identify the common characteristics of these attacks (assuming that the reader is aware of the details of the two attacks) and deduce what is necessary to stay safe in this era where war has acquired a new *character*. A lot of emphasis is placed in the media on the use of drones, which very richly deserve attention; however, this article deliberately avoids referencing this technology to provide a more comprehensive picture.

The most obvious observation is that both attacks relied on a commonly used product with commercial demand, utilised by the local population and devoid of any lethal features in their original design. While the utility of pagers in Lebanon and the wooden

cabins popular in the cold Siberian regions may not be similar, they are both presumed to be non-lethal in nature.

The ingenious and undetectable modification, or more accurately, the weaponisation of the product without any change to its physical appearance, was perfect in both cases and remained undetected by the agencies through which the product passed during its journey toward the intended target. The ingenuity of this modification was such that it utilised the limited space available inside the product to pack adequate lethality to deal with the target effectively. This ingenuity further extended to remote operation through secure and fail-safe communication, ultimately striking and triggering at the most vulnerable part of the target to maximise damage. The ease with which a non-lethal object was transformed into an object of destruction is the chilling reality that the world must confront.

Another aspect of commonality is the discreet and routine movement of the product through the supply chain without arousing any suspicion among the supply chain managers and handlers involved in the downstream transport of the product to the consignee. This aspect leverages the trust established among supply chain constituents and the inherent capacity of supply chains to deliver products with precision, at the right time, to the right consignee, in the right location.

The commonality between the two attacks also extends to the location and nature of the targets. The targets chosen for the attacks were not on the front lines but rather in the hinterland, which is easily accessible through the exploitation of supply chains. This capability creates the element of extreme surprise that such attacks enjoyed, along with the accompanying shock and awe, and intense media attention. Another obvious implication is that the perception of strategic assets being safe in depth locations, away from the front, during both peace and war, will now undergo a dramatic change. Every asset, regardless of its location, is vulnerable at all times, and it is something to get accustomed to.

The most striking aspect of the recent attacks is their asymmetric nature. The technology and equipment deployed are readily available at a low cost. The Ukrainians utilised one hundred seventeen pieces of hardware, each costing less than USD

2,000, along with easily accessible open-source software, and destroyed strategic assets worth over USD 7 billion. In terms of the cost-to-damage ratio, the damage exceeds 30,000 times the incurred cost, a ratio that is indeed intimidating[ii]. This calculation does not account for the likely expenditures that the Russians will now incur on monitoring the movement of goods within their borders; an effort that will take a significant toll on their economy. This asymmetry makes the newly evolved character of war appealing and is likely to be the first choice of Davids in all *David versus Goliath* contests; thus, it presents a strong case for Goliaths to prepare their defences accordingly. Furthermore, the Davids could be both state and non-state actors, which makes the situation even more grim[iii].

The planning necessary for executing such operations, as well as their execution, is extensive and time-consuming. The Israelis would have taken over a year to carry out the attack on Hezbollah. Ukraine, according to its own statements, took 18 months to execute the marvel. This operation required meticulous planning and a slow, deliberate deployment of the transformed product at the terminal end without attracting anyone's attention. Therefore, the attacks we are witnessing now were conceived in mid to late 2023, which is why the assertion that we are already past the inflection point is correct.

Perhaps the most concerning aspect is that the targets chosen in such attacks are strategic in nature. Axiomatically, low-cost non-lethal products moving in day-to-day commercial supply chains can be easily modified with ingenuity to cause substantial damage to invaluable and not easily replaceable strategic assets in depth. Additionally, if the strategic assets must be kept safe, their physical security would need to be reevaluated, as well as that of the products moving in the supply chains surrounding these assets.

The two attacks discussed above in generic terms are highly evolved supply chain attacks that not only target strategic assets but have also been used for strategic messaging. One must read the statements in the media to comprehend this. An assertion following the Ukrainian attack describes it as *titanic*. Zelenskyy wrote on his Telegram channel after the attack, “but these are Ukrainian actions that will

undoubtedly be in history books." Business Ukraine journal commented, "it turns out Ukraine does have some cards after all. Today Zelensky played the King of Drones."[iv]

The characteristics discussed above are revealing of what is to come in the times ahead. It is reasonable to assume that similar attacks are being planned and developed for use with new products at the time of writing of this article. The crucial question, therefore, is: How can nations defend against such attacks? How can they foil such an attack? It is apparent that conventional defence mechanisms and strategies are ineffective against such attacks. A new paradigm for defence that focuses more within the borders rather than on the borders may be a plausible solution. A new paradigm that keeps the strategic assets safe from low-cost, asymmetric attacks delivered through ordinary products moving in the supply chain. Key to this is investing in and developing supply chain intelligence, as well as establishing new methods to create trust among supply chain partners, so they collectively ensure that products moving through the supply chain are not altered at any stage.[v] Supply chain transparency, both during manufacture and in transit, is another issue that demands serious attention and effort. The global community must urgently prioritise attention to both supply chain intelligence and transparency and evolve methods that prevent the weaponisation of everyday items and the supply chain itself from being used as a means to deliver destructive payloads.

Disclaimer

The views expressed in this monograph are solely those of the author and do not necessarily reflect the opinions or policies of CENJOWS. The author affirms that this work is an original piece of scholarly research, has not been published or submitted for publication elsewhere (in print or online), and that all data, facts, and figures cited are appropriately referenced and believed to be accurate to the best of the author's

Reference

[i] M. A. Milley, “Strategic Inflection Point the Most Historically Significant and Fundamental Change in the Character of War Is Happening Now— While the Future Is Clouded in Mist and Uncertainty,” JFQ, vol. 3rd Quarter, no. 110, pp. 7-15, 2023.

[ii] Molloy, Oleksandra. Drones in Modern Warfare: Lessons Learnt from the War in Ukraine. Australian Army Occasional Paper No. 29. Canberra: Commonwealth of Australia, 2024. https://doi.org/10.61451/267513.

[iii] Sadık, Giray, ed. The Effects of the Russia-Ukraine War on Countering Terrorism. Ankara: Centre of Excellence Defence Against Terrorism (COE-DAT), 2025.

[iv] Johnson, Reuben. “Zelenskyy’s Drone Card: How Operation Spiderweb Impacts Russia’s Capabilities Going Forward.” *Breaking Défense*, June 3, 2025, 4:10 PM.

[v] S. Sethi, “Clausewitz, pagers, and the evolving art of supply chain attacks,” CLAWS, 2024 November 2024. [Online]. Available: https://claws.co.in/clausewitz-pagers-and-the-evolving-art-of-supply-chain-attacks/.