SYSTEMATIZING SUPPLY CHAIN WARFARE

PETER LAYTON

Airpower thinkers must reconsider attacks on the logistics support of modern military forces using a systems perspective centered on the operations and dynamics of an adversary's supply chain. Such a reassessment has become increasingly important, given the return of major war, the realization a protracted great power war may be possible, the Ukrainian war experience in terms of economic warfare and interdiction, the rise of heterogenous airpower, and the potential of affordable mass airpower. This analysis focuses on the target system—the contemporary supply chain—understood as a restricted complexity system type characterized by semi-openness, multiple causality, and dispersion. Incorporating key twentieth-century airpower theories including interdiction, industrial web, and economic warfare into a twenty-first-century systems theory approach can advance thinking about the contemporary application of airpower at the operational, strategic, and grand strategic levels.

There is an apocryphal saying that amateurs talk about strategy but professionals talk about logistics, the art of moving armies and keeping them supplied.[1] Unsurprisingly, when airpower first allowed military force to be easily applied beyond an enemy's front line, aircraft attacked an army's logistics. Since World War I though, the concept of logistics has changed.

For most of the twentieth century, businesses sought to keep their activities in-house; through vertical integration they could firmly control all aspects of their industrial processes. In the 1990s, however, many companies began shifting to horizontal integration, using extensive outsourcing and keeping only core functions in-house. The new concept of supply chains arose while logistics as an idea retreated to being a subset, mainly about activity administration within a company.[2] Today, modern supply chains are vast, complex, and global, and can be best understood using a systems perspective. Such supply chains are systems with a purpose that have a certain operating logic, which in itself creates sensitivities and vulnerabilities.

Dr. Peter Layton is a visiting fellow at the Griffith Asia Institute at Griffith University in Queensland, Australia.

1. Martin Van Creveld, *Supplying War: Logistics from Wallenstein to Patton* (Cambridge, MA: Cambridge University Press, 1977), 1.

2. Ronald H. Ballou, "The Evolution and Future of Logistics and Supply Chain Management," *European Business Review* 19, no. 4 (July 2007): 341, https://doi.org/.

These susceptibilities to deliberate interference have attracted increasing attention in recent years as geostrategic tensions have emerged. Sanctions to cut supply chains that quarrelsome states rely on for their military forces, technological advancement, or financial strength are now often used.[3] While Iran and North Korea have long been subject to purposeful supply-line obstructions, Russia's war in Ukraine now sees Russia having its supply chains for military equipment components being cut, requiring the country to seek ever more complex smuggling approaches and different, less-capable suppliers.[4] As a result, Russia's combat forces are impacted both quantitatively in being able to field less military equipment and qualitatively in needing to revert to using older, less effective military hardware.[5]

Ukraine, with the assistance of the West, has integrated economic warfare with the traditional method of interdiction, albeit constrained by political restrictions on taking the conflict deep into Russian territory. Ukraine has used high-mobility artillery rocket system (HIMARS) rockets, attack drones, and Storm Shadow cruise missiles to damage Russian military supply chains running through Ukrainian-occupied territory.[6] On the other hand Russia has been less constrained and has attacked defense industry sites, transport infrastructure, and supply depots across all of Ukraine.[7]

Applying Airpower in the Twenty-First Century

While the Ukraine war has reemphasized the importance to combat operations of constraining supplies, the conflict has also highlighted that airpower is now much

3. US Department of the Treasury (Treasury), "Treasury Sanctions Procurement Network Supporting Iran's UAV and Military Programs," press release, Treasury, April 19, 2023, https://home.treasury.gov/; Coco Feng, "China's Big Tech Firms Scramble for Advanced Chips amid US Sanctions and ChatGPT Craze, *South China Morning Post*, June 14, 2023, https://www.scmp.com/; and Treasury, "With over 300 Sanctions, U.S. Targets Russia's Circumvention and Evasion, Military-Industrial Supply Chains, and Future Energy Revenues, press release, Treasury, May 19, 2023, https://home.treasury.gov/.

4. Bohdan Miroshnychenko, "Contraband Tumor: How Russia Steals Military Technology and What To Do about It," Економічна правда, May 17, 2022. https://www.epravda.com.ua/; and Jeanne Whalen, "Sanctions Forcing Russia to Use Appliance Parts in Military Gear, U.S. Says," *Washington Post*, May 5, 2022. https://www.washingtonpost.com/.

5. Max Bergmann et al., *Out of Stock? Assessing the Impact of Sanctions on Russia's Defense Industry* (Washington, DC: Center for Strategic and International Studies, 2023), 3.

6. Isabel Coles and Daniel Michaels, "The Offensive before the Offensive: Ukraine Strikes behind Russian Lines," *Wall Street Journal*, May 17, 2023, https://www.wsj.com/; "Ukraine Rockets 'Significantly' Reducing Russian Attack Potential," Aljazeera, July 15, 2022, https://www.aljazeera.com/; Howard Altman, "Multiple Russian Fuel Depots Hit by Suspected Drone Attacks, Tempo Increasing," The Drive, May 4, 2023, https://www.thedrive.com/; and Jack Watling, "Putting Russia's Army in the Shadow of the Storm," Royal United Services Institute for Defence and Security Studies (RUSI) (website), May 15, 2023, https://rusi.org/.

7. Alistair MacDonald, "Ukraine's Arms Industry Survives Russian Onslaught to Hit Back, *Wall Street Journal*, May 1, 2023, https://www.wsj.com/; Jake Epstein, "How Ukraine's 'Lifeline' Runs Even as Russia Bombs It, According to a Man Fighting to Keep the Trains on Time," *Business Insider*, February 26, 2023, https://www.businessinsider.com/; and "Russia Says It Has Destroyed 70,000-Tonne Fuel Depot near Zaporizhzhia," Reuters, April 9, 2023, https://www.reuters.com/.

more heterogenous than in the last century. In wars today, air attacks can be carried out not just by crewed aircraft but also by short- and long-range cruise missiles, ballistic missiles, and uncrewed drones. The latter in particular are being used in significantly large numbers in Ukraine, reinforcing an emerging concept of uncrewed aerial systems returning a mass to air warfare lost as crewed aircraft become more costly and difficult to build. Incidentally, the emerging prospect of "affordable mass" airpower raises the question of how this could be used.[8]

The Ukraine war has further added to a growing belief that future wars might be protracted, perhaps by several years.[9] The longer a war lasts the greater the reliance on replacing equipment, as that employed at the start is lost through attrition or use. Looking to the future, the greatest geostrategic worry is a major war with China. Many suggest such a war would inevitably be prolonged, lasting well beyond the initial engagements.[10] There have long been arguments that supply chain warfare would play a significant role in such a conflict, with a particular focus on cutting China's globe-spanning supply chains.[11]

These various factors all combine to prompt an urgent reconsideration of supply chain warfare. Airpower has been used in such warfare before, especially in the great power wars of the first half of the twentieth century. These earlier concepts and experiences offer useful insights into what has and has not succeeded in previous conflicts. Collectively, they represent a body of work on which to build a reassessment, but this involves some significant changes to take account of contemporary supply chain concepts and a shift in the underlying paradigm about how the world operates.

Early twentieth-century airpower thinking often took a fairly reductionist approach, seeing the world as an analog, clockwork-like machine composed of many individual parts.[12] Since then, systems thinking has advanced and matured; such an approach takes a holistic view and examines a system's internal relationships rather than focusing on the constituent parts as standalone items. It is not that reductionist thinking has been replaced but that systems thinking offers another way to see the

8. Joseph Trevithick, "Affordable Mass Concept Driving Air Force's New Advanced Drone Initiative," The Drive, March 10, 2023, https://www.thedrive.com/.

9. Andrew F. Krepinevich, *Protracted Great-Power War: A Preliminary Assessment* (Washington, DC: Center for a New American Security, 2020).

10. Timothy R. Heath, Kristen Gunness, and Tristan Finazzo, *The Return of Great Power War: Scenarios of Systemic Conflict between the United States and China* (Santa Monica, CA: RAND Corporation, 2022); and Hal Brands, *Getting Ready for a Long War with China: Dynamics of Protracted Conflict in the Western Pacific* (Washington, DC: American Enterprise Institute, 2022).

11. Fiona S. Cunningham, "The Maritime Rung on the Escalation Ladder: Naval Blockades in a US-China Conflict," *Security Studies* 29, no. 4 (August 2020); Sean Mirski, "Stranglehold: The Context, Conduct and Consequences of an American Naval Blockade of China," *Journal of Strategic Studies* 36, no. 3 (June 2013); and Gabriel B. Collins and William S. Murray, "No Oil for the Lamps of China?," *Naval War College Review* 61, no. 2 (Spring 2008).

12. Steven M. Rinaldi, "Complexity Theory and Air Power," in *Complexity, Global Politics, and National Security*, ed. David S. Alberts and Thomas J. Czerwinski (Washington, DC: National Defense University, 2002).

world and especially those matters with significant human involvement. Modern US Air Force targeting concepts stress using target systems analysis.[13] Such an analysis involves identifying, describing, and evaluating the composition of an adversary target system to determine its capabilities, requirements, and vulnerabilities.[14]

Importantly, systems thinking has now shifted from being an abstract idea into a more tangible reality. Recent advances in artificial intelligence, including machine learning techniques, make it possible to create and run in near-real time large dynamic models of complicated systems able to provide useful insights into how these systems may react to various interventions.[15] This new tool is now available to help people reach optimum solutions to certain difficult problems. Airpower planners could use these to inform their supply chain warfare thinking when considering attack options.

Rather than examining emerging technologies or geostrategy, this article instead adopts a systems perspective focused on the target set. The target, rather than the means of attack or the context, forms the core of the discussion. The modern supply chain process of planning, sourcing, making, and delivering is encompassed within three disparate but related types of warfare—interdiction, the industrial web, and economic warfare. Moreover, these three approaches are each most useful at a different level of strategic thinking—operational, strategic, and grand strategic—when considering adversary supply chains as a target system set.[16]

Examining the issues at these different levels of war indicates that for supply chain warfare to be most effective and efficient, it may need to be conceptualized and waged more deeply than perhaps initially envisaged.[17] A decisive impact on supply chains may require interdiction, industrial web attacks, and economic warfare to be waged simultaneously in a coordinated manner.

Paradoxically, new supply chain technologies also suggest taking a comprehensive view. For example, additive manufacturing, the process of growing three-dimensional (3D) objects one layer at a time—colloquially termed 3D printing—offers the tantalizing possibility of manufacturing close to the front line, providing certain necessary items quickly without traversing long supply lines. But 3D printing still requires appropriate machines, facilities, and raw materials, and its proximity to the battlefield makes it much more vulnerable to air attack than distant supply sources. Ideas about

13. US Air Force, *Targeting*, Air Force Doctrine Publication (AFDP) 3-60 (Maxwell AFB, AL: Curtis LeMay Center for Doctrine Development and Education [LeMay Center], November 12, 2021), 42–43, https://www.doctrine.af.mil/.

14. Curtis E. Pinnix Jr., "Specialized Analytic and Targeting Study: A Methodology and Approach for Conducting Faster Full-Spectrum Targeting," *Joint Forces Quarterly* 103, no. 4 (4th Quarter 2021), https://ndupress.ndu.edu/.

15. Jennifer McArdle and Caitlin Dohrmann, "From Legos to Modular Simulation Architectures: Enabling the Power of Future (War) Play," *Mad Scientist Laboratory*, January 25, 2021, https://madsciblog.tradoc.army.mil/; and Lauren Speranza and Jennifer McArdle, "Five Ways Synthetic Environments Can Benefit NATO," *Defense News*, February 3, 2022, https://www.defensenews.com/.

16. Edward Luttwak, *Strategy: The Logic of War and Peace* (Cambridge, MA: Belknap Press, 1987), 69–71.

17. The author is indebted to an unknown reviewer regarding this reflection.

interdiction, the industrial web, and economic warfare then remain important but overlap and are drastically compressed.

Twentieth-Century Airpower

Interdiction

In 1917, then Major General Hugh Trenchard detailed an air campaign that focused on key targets: railways, railroad marshalling yards, bridges, supply depots, and road networks that moved men and materiel to the front lines.[18] The concept, known as interdiction, was developed further in a seminal book written by British Royal Air Force Wing Commander John Slessor, *Air Power and Armies*, which examined the operational level of war.[19]

Slessor, an instructor at the British Army War College at the time, argued airpower could seal off an enemy's forces, strangling them into capitulation.[20] In this, Slessor preferred supply interdiction of materiel and equipment over force interdiction, known in modern parlance as battlefield air interdiction. He argued airpower should maintain continuous air attacks as far to the rear of the army as possible, aiming not to destroy but instead to paralyze supply efforts and communication lines.

The practice of air interdiction in World War II revealed that interdiction needed to be a sustained operation requiring persistence and continual pressure. The characteristics of the enemy's lines of communication (LOC) greatly influenced the overall impact of an interdiction campaign. The length and type of the LOCs, the presence of enemy choke points, and concentration of supplies all determined the availability of high-payoff targets.

An outstanding example of World War II interdiction by Allied forces involved the lengthy LOCs connecting Japan to the Solomon Islands in 1942–43. The Solomons were on the very edge of the greatly extended Japanese wartime empire, more than 3,000 miles from Tokyo. When the US Marines landed on Guadalcanal to capture the airfield, the Japanese opted to make a major defensive effort that required sending additional troops and extensive resupply by ships. In the end, it was the Allied interdiction of shipping and not the actual fighting on the island that proved decisive in thwarting the invasion. Interrogated post-war, Lieutenant General Shuichi Miyazaki, chief of staff to the Japanese 17th Army at the time of the invasion, observed this:

> The biggest problem was the loss of ships. Actually the bombing of troops and troop concentrations on the ground were not much of a hindrance because,

18. Phillip S. Meilinger, "Trenchard, Slessor, and Royal Air Force [RAF] Doctrine before World War II," in *The Paths of Heaven: The Evolution of Airpower Theory*, ed. Phillip S. Meilinger (Maxwell AFB, AL: Air University Press [AUP], 1997), 45.

19. John Cotesworth Slessor, *Air Power and Armies* (London: Oxford University Press, 1936); and Michael Howard, "Marshal of the Royal Air Force Sir John Slessor and the Prevention of War," Medium, Royal Air Force Centre for Air and Space Power Studies (RAF CASPS), May 4, 2018, https://medium.com/.

20. Meilinger, "Trenchard, Slessor, and RAF," 62.

> although the bombing scared everybody and made lots of noise and had an effect on morale, the actual destruction was not very great. The biggest problem was the loss of our capacity to move these troops to the fighting areas.[21]

The scale of the interdiction's impact is well illustrated in the fate of Japan's 38th Division which was attacked in transit: of the division's 12,000 men, only 2,000 made it to Guadalcanal.

Similar problems beset Japanese forces fighting in Papua New Guinea. In the Battle of the Bismarck Sea, an eight-ship convoy transporting troops to Lae was attacked by Allied airpower; of the 6,900 troops on board only 1,200 were rescued from the sea by warships and only 850 made it to Lae. The interdiction campaign was so successful because it leveraged the structural factors of geography and the Japanese need to continue resupply efforts given their decision to keep fighting and not withdraw.

Interdiction today. The contemporary understanding of interdiction is that it is "an action to divert, disrupt, delay, or destroy the enemy's military surface capability before it can be used effectively against friendly forces or to achieve enemy objectives."[22] Hostile forces can be diverted away from critically important operational areas. Disruption can damage an adversary force's information flows, operational tempo, combined arms coordination, and cohesion. Delays can prevent the timely arrival of enemy forces on the battlefield and impact an adversary's ability to project power. Destruction harms the structure, function, or condition of a targeted entity, making it operationally useless.

Interdiction planning is important precampaign and then during the campaign as it is implemented and the adversary responds. An adversary will often change their intent, plans, and force posture to try to reduce the impact of interdiction efforts. Campaign plans need to be continually reassessed in terms of a particular operational context and the relative timing of actions within that context.

Industrial Web

In the 1930s, a different concept was developed concerning attacking adversary supply systems. The US Army Air Corps Tactical School proposed attacking a nation's industrial web. This was not an indiscriminate attack but rather a focused one against identified "key nodes" that "would unravel the intricate web of a modern industrial economy."[23] A 1938 textbook used for the school's Air Force course explained this concept:

---

21. Headquarters US Army, *United States Strategic Bombing Survey*, "Effect of Allied Air Activity," Serial No. 497, Report No. 2-o(48), USSBS Index Section 8 (San Francisco, CA: Military Analysis Division, December 1945): 4, https://dl.ndl.go.jp/.

22. Chairman of the Joint Chiefs of Staff (CJCS), *Joint Interdiction*, Joint Publication (JP) 3-03 (Washington, DC: CJCS, September 9, 2016), ix.

23. Tami Davis Biddle, "British and American Approaches to Strategic Bombing: Their Origins and Implementation in the World War II Combined Bomber Offensive," *Journal of Strategic Studies* 18, no. 1 (March 1995): 111, https://doi.org/.

> The economic structure of a modern highly industrialized nation is characterized by the great degree of interdependence of its various elements. Certain of these elements are vital to the continued functioning of the modern nation. If one of these elements is destroyed the whole of the economic machine ceases to function. . . . Against a highly industrialized nation, such action may produce immediate and decisive results.[24]

In 1939, the British Air Ministry directed a series of "bottleneck" studies to determine the crucial elements within important sectors of the German economy. Bottleneck target sets were considered those of major importance to a nation's military, with most production concentrated in only a small number of facilities and with very limited spare production capacity inside or outside the country. The manufacturing was done using machinery unable to be quickly repaired or replaced and incapable of quick dispersal without significant production loss. Other factors of concern were the level of reserve stocks held by the adversary, the possibility of substitution, the susceptibility to air attack, and the potential of time-compression problems for the adversary military.[25]

Early in the war, the Royal Air Force did not have the technical capabilities to pursue a bottleneck campaign. The US Army Air Forces, however, entered later and with different capabilities, and adopted the Air Corps Tactical School's industrial web concept. In the Air War Plans Division's first plan (AWPD-1) developed prewar, the major targets selected were the electric power system, transport and particularly the railway network, and the petroleum industry. When the United States entered the war in 1942, the plan was modified into AWPD-42, which added aluminum and synthetic rubber, the latter based on the false assumption that the German army was as motorized as the US Army.[26]

In 1944, a bureaucratic battle erupted between proponents of interdiction versus industrial web attacks. With a need to support Allied amphibious landings in Normandy in mid-1944, some strategists argued interdiction attacks on connections—in this case railways and railway marshalling yards—would be more efficacious than bombing industrial web nodes, in particular oil refining plants. In the end, bridges, proving easier to destroy than anticipated, replaced marshalling yards in interdiction targeting, while attacks on oil plants had impacts on German military positions measured in days, not months, as planners had originally assumed.

The two target types—interdiction and industrial web—were to some extent related. The combination of attacks helped to isolate Normandy Beach. By forcing the Luftwaffe to defend the oil refineries and in so doing thus be destroyed, it also helped to

24. "Air Warfare" section, *Air Force* [textbook], Air Corps Tactical School, February 1, 1938, USAFHRC, decimal file no. 248.101-01, as qtd. in Biddle, "British and American Approaches."

25. Scott E. Wuesthoff, *The Utility of Targeting the Petroleum-Based Sector of a Nation's Economic Infrastructure* (Maxwell AFB: AUP, 1994), 4–8.

26. R. J. Overy, *The Air War, 1939–1945* (London: Papermac, 1980), 107.

deliver a major strategic blow to German military capabilities.[27] The wartime commander of Germany's fighter forces, Adolf Galland, observed that "the raids of the Allied air fleets on the German petrol supply installations [were] the most important of the combined factors which bought about the collapse of Germany."[28]

Industrial web today. Modern conventional warfare requires not only adequate military forces, but also advanced economic infrastructures capable of supporting these forces. Such infrastructures provide large vulnerable targets susceptible to enemy air attack. For industrial web attacks, there are two alternative but potentially overlapping approaches available.

In a reductionist approach, the adversary economy is dissected into its component parts with specific parts then attacked in isolation. This steps through analyzing a national economy, determining a critical industry, and then finding the key bottlenecks within it, the destruction of which would damage the critical industry's functioning and outputs. The more systemic approach focuses on the interconnections between the elements of an economy, identifying these and then exploiting critical linkages. In the first approach, individual target sets are attacked, while in the second, key points across different target sets are attacked.[29] In both approaches, it is important not to view the adversary industries as a static set of targets; these industries are constantly changing in response to demand and supply factors.

One post-World War II scholar argued attacks on what were considered critical industries would not usually bring strategic success as the adversary could often substitute one product for another and fill the gaps created.[30] "It is not the type of good, but the type of use that distinguishes a necessity from a luxury."[31] Targeteers should accordingly choose an industry sufficiently large and unique that its replacement would be costly. They would then attack not only that industry but also the industries and activities that would substitute for it when it is destroyed.[32]

As one example from World War II suggests, the choice of industry is crucial to target system analysis. At the time, the ball bearing industry appeared to be a key node, as ball bearings seemed to be critical components of Germany machinery and equipment and production was concentrated within a few factories. Allied air attacks were undertaken at great cost in lost aircraft and crew and did cause significant damage. Yet the Germans substituted plain bearings and devised work-arounds, later

27. W. W. Rostow, *Pre-Invasion Bombing Strategy: General Eisenhower's Decision of March 25, 1944* (Austin: University of Texas Press, 1981).

28. Adolf Galland, *The First and the Last* (New York: Bantam Edition, 1978), 266.

29. Steven M. Rinaldi, *Beyond the Industrial Web: Economic Synergies and Targeting Methodologies* (Maxwell AFB, AL: AUP, 1995), 1–2.

30. Mark Harrison, "Economic Warfare and Mançur Olson: Insights for Great Power Conflict," CEPR: Centre for Economic Policy Research, March 25, 2022, https://cepr.org/.

31. Mançur Olson Jr., *The Economics of the Wartime Shortage: A History of British Food Supplies in the Napoleonic War and in World Wars I and II* (Durham, NC: Duke University Press, 1963), 9.

32. Mançur Olson Jr., "The Economics of Target Selection for the Combined Bomber Offensive," *RUSI Journal* 107, no. 628 (1962): 314, https://doi.org/.

claiming that no military "equipment was ever delayed [in delivery] because bearings were lacking."[33] Choosing a target thus involves properly identifying a critical industry and deeply considering how an adversary may respond.

Economic Warfare

In 1939, with major war looming, the United Kingdom created the Ministry for Economic Warfare, later to be matched in the United States by the Board of Economic Warfare.[34] Combining the long history of British naval trade blockade operations and the new technology of airpower, the first official definition of economic warfare declared:

> The aim of economic warfare is so to disorganize the enemy's economy as to prevent him from carrying on the war. Its effectiveness in any war in which this country may be engaged will vary inversely with the degree of self-sufficiency which the enemy has attained, and/or the facilities he has, and can maintain, for securing supplies from neighbouring countries, and directly with the extent to which (i) his imports must be transported across seas which can be controlled by His Majesty's ships, (ii) his industry and centres of storage, production, manufacture and distribution are vulnerable to attack from the air, and (iii) opportunities arise from interfering with exports originating from his territories.[35]

Conceptually, economic warfare differed from attacking a state's military capabilities and, while it could overlap with such attacks, it could also be waged independently.

Economies are complex systems composed of a number of infrastructure elements interconnected in a myriad of ways and including electrical grids, petroleum and oil distribution networks, and telecommunications systems. As a result of this connectivity, an attack on one infrastructure element would influence the others to varying degrees. When targeting an economy, this connectivity and its intrinsic downstream effects could be leveraged.[36]

In this, to consider a national economy as static is misleading; instead, active adjustment to change is normal. Strategists were long familiar with creating tactical supply problems for the adversary, but airpower in World War II could now create a strategic supply problem that was new.[37] Strategic supply involved the capacity of a nation's entire economy to supply its military forces and continue the war. In a tactical supply situation, no quantity of extra supplies of the wrong kind could be substituted for the missing items.

---

33. Olson, "Target Selection," 309.

34. Lois H. Gruendl, *The Impact Of Offensive Economic Warfare on the Operational Commander* (Newport, RI: Naval War College, 1995), 8.

35. William Norton Medlicott, *The Economic Blockade, Vol. 1* (London: His Majesty's Stationery House and Longmans, Green and Co., 1952), 1.

36. Rinaldi, *Beyond the Industrial Web*, v.

37. Olson, "Target Selection."

In contrast, in a strategic supply situation most of what was missing could be replaced provided a nation was willing and able to substitute enough production of other things to secure it. To avoid this, economic warfare proposed that a major bottleneck in the overall economic system should be destroyed with further attacks undertaken to close off the possibilities of substitution.[38]

Economic warfare today. At its core, economic warfare is a cumulative strategy where small gains each day add up.[39] It greatly relies on accurate and continuing intelligence to identify strategic raw materials, sources of procurement, available stockpiles, rates of usage, potential substitutes, and key industrial sites. But poor intelligence, an inadequate application of force, and the failure to maintain ongoing pressure can lead to poor results.[40] Even so, a national economy is large and difficult to fully understand. As one analyst notes, "the art of waging economic warfare is imprecise and unpredictable."[41] There is inevitably some degree of trial and error in waging such warfare.

On the other hand, the global proliferation of digital technology has revolutionized the means of economic warfare. Cyberattacks on an adversary's economy can be conducted worldwide with no constraints concerning geographic sanctuaries. Such attacks can be preplanned with malware installed prewar awaiting activation, can be low cost, and can capture financial assets and not draw off kinetic assets from being used elsewhere.

Contemporary Supply Chains

Process

The modern supply chain process involves four basic elements: plan, source, make, and deliver. The process may be usefully defined as "all the activities involved in delivering a product from raw material through to the customer," including sourcing the materials and parts, manufacturing and assembly, warehousing and inventory tracking, order management, distribution, delivery, and monitoring the activities by information systems. Management of the supply chain process "coordinates and integrates all of these activities into a seamless process."[42]

Structure

There is a vertical dimension to this as supply chains usually have different tiers. Tier-1 suppliers conduct business directly with the company that undertakes the final assembly. In the aerospace market, this company is often termed the original equipment

38. Olson, "Target Selection," 310–14.

39. J.C. Wylie, *Military Strategy: A General Theory of Power Control* (Sydney: Australian Naval Institute Press, 1967), 26.

40. Gruendl, *Offensive Economic Warfare*, 10–11.

41. Gruendl, 3.

42. Rhonda R. Lummus and Robert J. Vokurka, "Defining Supply Chain Management: A Historical Perspective and Practical Guidelines," *Industrial Management & Data Systems* 99, no. 1 (1999), 11.

manufacturer (OEM). Beneath this, tier-*n* suppliers serve as the sources of primary materials and component parts for the higher tiers—for instance, tier-2 suppliers are the suppliers or subcontractors for tier-1 suppliers, tier-3 for tier-2 suppliers, and so on.

The supply chain concept drives companies to become highly specialized; as a result, many supply chains contain a multitude of tiers. Subordinate tiers are connected vertically; generally only the tier-1 suppliers are linked horizontally to the OEM. Consequently, supply chains represent not only a linear chain of one-on-one business relationships but also a downward web of multiple business networks and relationships. Moreover, the overall supply chain is entangled with its environment and continuously evolving with it. In a broad conceptual sense, the supply chain is a decentralized network of several layers all the way down the various interacting tiers.[43]

Command and Control

Supply networks are social-technical systems with human and nonhuman elements. Suppliers, manufacturers, retailers, and customers work together through partnerships or alliances; each has their specific function in the system. An environment of intense interaction is created driven by exchanges of material, financial, and informational resources including knowledge.[44] Along the supply chain, there is a forward flow of goods and a backward flow of information.[45]

The functioning of supply chains involves dispersed authority. Although the details of the overall supply chain may be unknown to any single company, individual companies engage in localized decision-making: they select their suppliers and ensure product delivery to buyers. Control is generated through simple behavioral rules that operate based on local information.[46] Given this, supply chains inherently favor stability and try to maintain their configuration in response to external disturbances. But at some point, a cascade of changes may be triggered that leads to system-wide reconfigurations.

Type of System

Generic supply chains can be perceived as restricted complexity systems in having semi-openness, multiple causality, and dispersed authority. [47] Semi-openness is being able to draw on resources outside the system to compensate for internal disruption, but only those resources that have a dual civil-military function. Most modern military

43. Paul Baran, *On Distributed Communications: I. Introduction to Distributed Communications Networks, Memorandum RM-3420-PR* (Santa Monica, CA: RAND Corporation, 1964), 1–2.

44. Jamur Johnas Marchi, "Understanding Supply Networks from Complex Adaptive Systems," *BAR: Brazilian Administration Review* 11, no. 4 (October–December 2014): 446, https://doi.org/.

45. Amit Surana et al., "Supply-Chain Networks: A Complex Adaptive Systems Perspective," *International Journal of Production Research* 43, no. 20 (2005): 4239, https://doi.org/.

46. Surana et al.

47. Malte Brosig, "Restricted Complexity: A Middle Path between Postmodern Complexity Theory and Positivist Mainstream IR," *International Studies Review* 22, no. 4 (December 2020): 1015–19, https://doi.org/.

equipment requires specific components to operate and be repaired, and these can only come from particular supply sources. Supply chains have multiple causality in that supply solutions may come from multiple sources and through multiple pathways. Dispersed authority means there is no single directing authority; instead nodes communicate and coordinate among themselves to ensure inputs are received when the nodes need them and outputs are pushed into the supply chain when requested by other nodes.

Problems

Contemporary supply chains have some inherent problems. The first is that they can be brittle. This fragility arises from their opaqueness to most participants, the presence of single points of failure, and driven by the quest for economic efficacy, their high degree of complexity and interconnectedness. The more complex the supply chain, the greater the possibility it might fail in one or more of its functions. Still, this is only a possibility, as product substitutions and work-arounds may be viable, as mentioned earlier.

The second problem is their geographic spread, which is often worldwide. The final assembly of many products often requires materials from an assortment of manufacturers across the globe. Supply chains can then be subjected to distant unexpected events and geopolitical tensions that can quickly create outsized impacts. The third problem can be a lack of vendor diversity. Products that require materials from a certain region or a single source are at greater risk for disruption. A fourth issue is limited transparency. The companies involved rarely understand the full scope of their supply chain and so have trouble taking early corrective actions to effectively remedy looming disruptions. Contingency planning can be particularly difficult.[48]

A fifth issue is that information feedback in the system is often slow relative to the rate of changes occurring in the system. The system has a specific process to achieve the desired output; if disruptions happen too quickly for the control mechanism to keep up, outputs will markedly fluctuate as the system fractures and becomes internally disorganized.

The last problem is the so-called bullwhip effect, where one company's actions impact other companies along the supply chain given their interdependency. A small change in the downstream supply chain can then cause amplified effects in the upstream supply chain phases. The bullwhip effect may be caused by both sudden changes in demand forecast or unexpected scarcity, which is when the supply chain offers less than what is required at some stage in the chain, leading downstream companies to abruptly start rationing their products.[49]

All these issues mean that supply chains need to be managed. Ideally, supply chain management integrates all process activities seamlessly, with the entire process viewed

48. Megan Lamberth et al., *The Tangled Web We Wove: Rebalancing America's Supply Chains* (Washington, DC: Center for a New American Security, 2022), 9.

49. Marchi, "Understanding Supply Networks," 448.

as a single large system.[50] The reality is often less expansive, with supply chain management generally limited in its scope. The most likely place for such management is between the firm undertaking final assembly and its tier-1 suppliers.[51] Supply-chain management now increasingly relies on information technology.

Supply Chain Warfare Campaign Planning

Attacking a contemporary supply chain involves four considerations: system analysis, the objective, leverage points, and the new equilibrium the attack will establish.

Analysis

The first step is to analyze the supply chain system by identifying the key nodes, flows and relationships, and the feedback mechanisms that hold the system together. One study on targeting processes determined there was a compelling need to understand the selected target system's complexity, its adaptation processes, and the role of feedback loops in making the system robust.[52]

To gain the required understanding of a system, one systems theorist outlines several useful steps: "get the beat of the system"; create a structural diagram and use it to verify system operation; assess not just the quantifiable aspects but the qualitative as well; understand the feedback loops that keep the system within certain parameters; examine the forces and structures that help the system run itself; determine where the responsibilities lie within the system; and lastly, understand a system's full complexity rather than try to oversimplify it.[53]

Objective

The campaign objective may vary depending on the impact that is sought. At the operational level of war, supply chain warfare might focus on supporting the activities of other friendly military forces. This might draw on interdiction thinking and be phrased as actions to divert, disrupt, delay, or destroy an adversary's military capabilities as they seek to gain their objectives. In the modern era the focus is not on supporting land forces as in some World War II campaigns but rather supporting and acting across all domains. Yet, as with traditional interdiction, supporting friendly forces in this way relies on the adversary actively using up supplies they need to quickly replenish.

---

50. Barrie Michael Cole, *Supply Chain Optimization under Uncertainty: Supply Chain Design for Optimum Performance* (Wilmington, NC: Vernon Press 2014), 4.

51. Ronald H. Ballou, "The Evolution and Future of Logistics and Supply Chain Management," *Produção* 16, no. 3 (December 2006): 341, https://doi.org/.

52. Andrew Hoffmann, Systems-Based Targeting (master's thesis, UNSW Canberra, August 2019), 111, https://doi.org/.

53. Donella H. Meadows, *Thinking in Systems: A Primer*, ed. Diana Wright (London: Earthscan, 2008), 170, 194.

At the strategic level, industrial web approaches might aim to shorten the duration of the conflict by attacking key supply chain nodes critical to particular industries supporting an adversary's armed forces. There is again a reliance on the adversary having suitable vulnerabilities that could be exploited; for example, the adversary might not be industrialized or might instead rely extensively on foreign support.

At the grand strategic level, economic warfare concepts could be drawn upon to guide disrupting the supply chains of industries necessary to sustaining an adversary's national power. This is much broader than degrading just an enemy's military power, would take longer to achieve, and would have a longer-lasting impact. This objective shades into war termination, in that an adversary's power might be purposefully reduced well into the post-war period.

Leverage Points

Ways suggested to improve a system's performance can be reversed to suggest ways to diminish its performance. This becomes a hunt for the critical variable, the so-called leverage point where a purposeful disruption in the way the system works will produce large changes in the system's output. In this, the term "leverage point" is a little confusing as while it relates to a particular part of a system, it actually seeks a change in system dynamics. The intent is to turn the way a system works against itself so that the effect of a disruption is magnified. This becomes apparent when considering two broad leverage types:

- **Physical leverages**. Using physical leverages includes attacking so as to drive the system outside its designed operating parameters; sharply reducing the stabilizing buffers—the system's internal material stockholdings kept at each step—that keep the system correctly flowing; attacking the system's structural arrangement to exploit physical limitations and bottlenecks; and causing delays in the feedback loops that are critical determinants of system behavior and that can cause system oscillations.[54]
- **Information and control leverages**. Using information and control leverages includes attacking the balancing feedback loops, in particular the accuracy and rapidity of monitoring, the quickness and power of response, and the directness and size of corrective flows; creating a runaway reinforcing feedback loop that leads to system destruction; damaging information flows so system managers cannot accurately control the system; attacking the internal self-reorganization devised to try to keep the system functioning while under attack; decapitating key control nodes; and if feasible, exploiting the different and dissimilar norms and identities of the diverse human staff across the system.[55]

54. Meadows.
55. Meadows.

The leverage points noted are system generic and now need to be considered in terms of the restricted complexity type of systems associated with supply chains. In the plan, source, make, and deliver supply chain system process there are numerous entry points at which kinetic or virtual pressure can be applied. These include sourcing raw materials and parts, manufacturing and assembly, warehousing and inventory management, distribution and delivery, and monitoring activities through overarching information systems. In this, the more complicated the supply chain, the greater its possible fragility and vulnerability to disturbance. Depending on its geographic spread, however, only some elements of the supply chain might be accessible and susceptible to physical attack. On the other hand, cyberattacks can usually be undertaken anywhere that information systems are used.

A factor in analyzing a supply chain is vendor diversity. If components are available from many sources, then this is not a critical step in the manufacturing process. On the other hand, if some components originate from only one supplier, then that node may present a systemic vulnerability. In this examination, the shape of the network in being decentralized may reveal exposed connections; there will be a choice between attacking the assembly node, the tier-1 suppliers, the tier-*n* suppliers, or combinations of these.

Such analysis makes an assumption that final assembly nodes are likely to be obvious to locate but in some way harder to be operationally impaired, whether by robustness, redundancy, or being defended. On the other hand, the various tier-1 and then tier-*n* suppliers will be progressively more difficult to pinpoint but be less resilient than an assembly node and, in generally being geographically dispersed, be less defended (if at all). Where pressure should be applied across the plan, source, make, and deliver process might vary with the objective of the supply chain warfare campaign.

Operational level. At the operational level, with its interdiction background, the deliver part of the process is stressed. This involves attacking warehousing, inventory management, distribution, delivery, and information systems. The campaign is then particularly shaped by the characteristics of the enemy's LOCs, including their length and type, the presence of choke points, and the concentration of supplies along the LOCs.

Accordingly, in terms of system leverages, the stabilizing buffers and the system's structure and node interaction represent key points for attack. On the other hand, the balancing feedback loop lever can be exploited to ensure adversary commanders keep pushing more and more supplies forward, driven by battlefield imperatives but increasingly providing multiple high-value targets and target sets for attack.

The World War II case of air and naval attacks on Japanese transport ships heading to the Solomon Islands across long, exposed, effectively indefensible LOCs was noted earlier. In a more recent example in Russia's war in Ukraine, the reliance by Russian artillery units on large ammunition storage dumps some 30 kilometers behind the

front line proved a significant vulnerability.[56] In being connected to railway lines, the storage dumps saw a rapid distribution by truck from them to the artillery units, which offered maximized efficiency, but this LOC relied on the Ukrainian military's inability to strike them, and that changed.

Strategic level. At the strategic level with industrial web approaches, there are distinct alternatives. The reductionist approach where key bottlenecks in a critical supply chain are attacked to create relatively swift results suggests a focus on the make part of the supply chain process. Accordingly, the stress might be on attacking the final assembly nodes of the chosen critical supply chain, even if these may in time be able to be replaced.

Another option is to damage one or more tier-1 suppliers in the chosen critical supply chain, accepting that the impact from this may be delayed but might be more enduring. The tier-1 suppliers actually make components; whereas, often the final assembly node is just that. Cutting the manufacture of an important component will not only affect final equipment assembly processes but may also affect sustainment of the in-service equipment if the component is needed in maintenance activities.

The alternative, more systemic approach focuses on key points across different target sets and suggests attacking selected tier-2 nodes across several industries. Such tier-2 attacks will impact several tier-1 nodes and then roll on to disrupt the final assembly nodes. The impacts will be relatively slow to be felt but will occur across the complete defense industry supply chain, depending on which nodes are targeted.

Considering system leverages, the main area for attacks is thus the interaction between the various levels in the chosen critical item chain, which is principally between the final assembly point and the tier-1 suppliers, and possibly down further into some selected tier-2 suppliers. To reinforce this disruption to supply, selected stabilizing buffers holding important components awaiting the final assembly phase might also be usefully attacked. Attacking these points will interrupt and delay the overall critical item system production process and cadence. In this, efforts could be made to reinforce and deepen the system oscillations caused by the attacks.

Additionally, it may be particularly advantageous to attack the information flows so decisionmakers have trouble understanding the scope of the problems arising and devising appropriate restructure work-arounds. In this, there will be balancing feedback loops brought into play that will try to introduce substitutes for those components made unavailable because of the attacks on the critical tier-1 and -2 suppliers. Attention should be paid to monitoring such systemic innovation and actions taken to negate it.

Grand strategic level. At the grand strategic level, the intent is diminishing the adversary's national power through choosing an industry sufficiently large and unique enough that its replacement will be costly, and then attacking not only that industry but also the industries and activities that serve as its substitute for when it is destroyed. This

56. Mykhaylo Zabrodskyi et al., *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022* (London: RUSI, 2022), 42–43.

suggests attacking the several tier-1 suppliers in the chosen industrial supply chain and then multiple tier-2 suppliers in the possible substitute product supply chains.

In this scenario, there is the issue noted earlier of triggering larger changes in overall supply chain system behavior. Economies are complex systems composed of a number of infrastructure elements interconnected in a myriad of ways, including electrical grids, petroleum and oil distribution networks, and telecommunications systems. As a result of this connectivity, a comprehensive attack on one infrastructure element will influence the others to varying degrees. When targeting an economy, this connectivity and its intrinsic downstream effects can be leveraged. Removing major infrastructure nodes or tier-1 suppliers within the national infrastructure supply chain network, such as within the petroleum distribution supply chain, will trigger systemic change. Supply chains are entangled with their environment and rely on interconnections to function; being unable to connect will create the need to change.

There are options beyond the physical given that supply chains are social-technical systems with human elements. Supply chains need to be managed, and because of this there is increasing reliance on information technology. This is an area where cyberattacks might be used to confuse, perplex, or deceive the supply chain managers.

Such attacks might be able to be focused in that the most likely place for such management is between the firm undertaking final assembly and its tier-1 suppliers. The tier-*n* suppliers are instead most likely coordinating themselves under local control. Such dispersed authority gives some useful system resilience, but as these suppliers operate alone in a series of islands, an attack of this nature can create a fragmented system if the tier-1 supplier is affected.

Given a supply chain involves a backward flow of information to ensure a forward flow of goods, a cyberattack can adversely seriously impact system performance. A well-known cause of instability in a supply chain is that the information feedback in the system is slow relative to the rate of changes occurring across the system. On the other hand, a bullwhip effect may be caused if the cyberattack causes confusion by seemingly creating a sudden change in forecast demand or an unexpected scarcity.

Considering system leverages, the main area for attacks might be the structure, that is the critical tier-1 and tier-2 suppliers, with more emphasis on the latter. The intent is to cause disruption at the national economic system level, not in a specific critical industry's system, as in the industrial web. In a way it is systems all the way down, with systems thinking applied at different levels of granularity from the national to the individual firm level. Disruption might be reinforced by attacking selected stabilizing buffers holding critical components, although this may now be mainly at the tier-2 level. Attacking these points will again interrupt and delay the overall system production process and cadence, creating systemic oscillations.

At the national level, maintaining useful information flows will be problematic; there will be significant amounts of data but filtering out critical factors for decision-makers to take action on will take time. These information flows will be particularly important pressure points to attack with potentially high payoffs.

A New Equilibrium

As a system, a supply chain responds to disturbances, whether caused by internal or external influences. Supply chains may internally respond by using any economic slack, substitution, reallocation, reengineering, reconstitution, and increased productivity. There are also external actions that may be taken, including stockpiling, rationing, importing, smuggling, disposing, hardening assets, and active defense.[57] As noted, a small change downstream can cause amplified effects upstream through the bullwhip effect.

An attack will push the system into a new equilibrium that may be positive or negative depending on the objective sought. This is a key point that taking a systemic view makes apparent. Before waging supply chain warfare, target system analysis will need to determine what this new equilibrium may be; if it may be positive the planned campaign will need to be rethought.

Conclusion

The reductionist approaches of the interwar period's airpower thinkers are anachronistic in a time where system approaches are favored. Yet with system approaches, no one type of system is appropriate for all varieties of targeting problems. The restricted complexity system type, characterized by semi-openness, multiple causality, and dispersed authority can be used when considering supply chain warfare.

Supply chain networks are social-technical systems with human and nonhuman elements. Suppliers, manufacturers, retailers, and customers work together through partnerships or alliances, each with a specific systemic function. An environment of intense interaction is created, driven by exchanges of material, financial, and informational resources including knowledge.

Where pressure might be applied varies with the objective. At the operational level of war, with its interdiction background, the delivery part of the supply chain process is stressed. At the strategic level with industrial web ideas, the stress might be on attacking the final assembly node of the chosen critical supply chain, even if it may in time be able to be repaired or replaced. Another option is to damage one or more tier-1 suppliers in the selected critical supply chain, accepting that the impact from this may be delayed but might be more enduring. At the grand strategic level involving damaging the overall national economic system, consideration might be given to attacking several tier-1 suppliers in the chosen industrial supply chain and then multiple tier-2 suppliers in possible substitute product supply chains.

Across all three supply chain options the generic system leverages are similar but the specifics vary. The leverages are the system's structure and interaction, selected stabilizing buffers holding critical components, and information flows. In addition, in the interdiction case the balancing feedback can be exploited to ensure adversary commanders keep pushing more and more supplies forward, and so provide multiple

57. Pat A. Pentland, *Center of Gravity Analysis and Chaos Theory* (Maxwell AFB, AL: AUP, 1993), 35.

high-value targets and target sets for attack. In contrast, in the industrial web and the national economic system cases, an adversary might bring balancing feedback loops into play to try to introduce substitutes for components made unavailable because of attacks; attention should be paid to monitoring for such systemic innovation and actions taken to negate it.

Supply chain systems have long been seen as suitable for air attack. Using a systemic perspective allows an understanding of enemy supply chains and of where to attack to maximize the damage done in terms of cutting system performance and output. Such analysis is gaining increasing relevance given the return of major, protracted war, the impact of economic warfare, recent successful interdiction of Russia's combat supply lines by Ukraine, the rise of heterogenous airpower, and the potential of affordable mass. Airpower thinkers should reconsider supply chain warfare. **Æ**