

SCENES
from the
ATLANTA FOREST

```

graph TD
    S1[Supplier] --> S2[Supplier]
    S3[Supplier] --> S4[Supplier]
    S3 --> S5[Supplier]
    S2 --> S6[Supplier]
    S4 --> S7[Supplier]
    S5 --> S7
    S6 --> M[Manufacturer]
    S7 --> M
    S7 --> M
  
```

```

graph TD
    Manufacturer[Manufacturer]
    S1[Supplier]
    S2[Supplier]
    S3[Supplier]
    S4[Supplier]
    S5[Supplier]
    S6[Supplier]
    S7[Supplier]
    S8[Supplier]

    Manufacturer --- S1
    Manufacturer --- S2
    Manufacturer --- S3
    S1 --> S4
    S1 --> S5
    S2 --> S5
    S2 --> S6
    S3 --> S6
    S3 --> S7
    S4 --> S8
    S5 --> S8
    S6 --> S8
    S7 --> S9
    S8 --> S9
  
```


Studying the enemy to identify vulnerabilities enables a quality of action, but *putting that knowledge into practice* is what makes it truly consequential. What are the current obstacles to anarchists developing a capacity for action on a significant scale, organized in small autonomous groups that can coordinate around a particular focus? In other words, what needs to happen for more anarchists to *establish the necessary skills and a certain routine for attacking identified vulnerabilities*?

Only by fostering an incisive quality of action can we hope to bring the factories of death to a standstill, to disrupt the infrastructure of war, and more broadly, to make meaningful contributions to the social upheavals on the horizon. The task at hand is not straightforward, but that does not make it any less necessary.

A recent text outlining a path for developing action capacity¹ concludes that “studying the vulnerabilities of domination” also needs attention. If a capacity for destruction is present, then the question naturally arises of how to aim it so that this destruction hits where it hurts. Let’s imagine what such an approach might entail by turning our gaze to a central pillar of global power and counterinsurgency: the U.S. “defense industry.” Anarchists and other rebels based in the U.S. are well-placed to strike at its war machine—the ‘60s saw a prolonged social upheaval driven primarily by this objective, and in the many years since, anarchists here have occasionally moved beyond opposing war to attacking it. The current genocide in Palestine has heightened social tensions against U.S. militarism, though the actions of anarchists in this moment have mostly had little impact on their targets and not contributed much to the popular imaginary of how militarism can be attacked. What could equip anarchists to carry out more significant strikes, to hone a quality of action that goes beyond the symbolic? To this end, the proposal put forward by “Fragments for an Insurgent Struggle Against Militarism and the World that Needs It”² deserves discussion: to focus on well-conceived attacks that target vulnerabilities in the production and infrastructure of war.

Breaking the links in the chain

The production of war starts here: the U.S. is by far the world’s largest arms exporter. Of SIPRI’s “Top 100 Arms-Producing and Military Services Companies,” 42 are based in the U.S., accounting for 51% of total global revenues. Most visible are

1 <https://scenes.noblogs.org/post/2024/02/22/developing-action-capacity-a-path/>

2 <https://actforfree.noblogs.org/2022/04/10/publication-war-against-war/>

the factories that churn out arms, ammunition and other war equipment. Less visible are the supply chains that transform raw materials into the components the factories need (production stage supply chains) or transport the finished product into the hands of States (distribution stage supply chains). *"Fragments for an Insurgent Struggle..."* proposes to focus destructive attention on the upstream supplier bottlenecks inherent in high-tech production, an industry "dependent on numerous expensive and difficult-to-obtain resources," rather than on the well-secured assembly plants:

Arson attacks on the vehicles of arms companies and their suppliers, as well as on the vehicles of the logistics companies that transported their war material, etc., as well as a perhaps even larger war fronts ever came to a standstill in the process. The interruption of production was too minor, the sabotage of logistics too insignificant. Nothing that could not have been made up by an additional night shift. And the financial damage? Well, let's say that the management of these companies make calculations in other dimensions.

It is by no means my intention to talk down these attempts at intervention, to discourage people from attacking even when the enemy seems overwhelming and one's own room to maneuver seems too small in comparison, one's own resistance too insignificant. None of this is a reason for me to refrain from attacking. Rather, I think it is worthwhile to reconsider established strategies from time to time and, if necessary, to revise them when it becomes apparent that one's actions within them are largely ineffective or becoming predictable.

infrastructure of war. Their words are no less relevant here:

We encourage people to make their own analyses of the military-industrial complex, its raw materials and its logistics, with no less than its efficient sabotage in mind. We feel the lack of such analysis all the more sharply because we believe that our ability to fight domination (and its wars) is irrevocably dependent on knowing its infrastructures, understanding the mechanisms that make them function and, not least, establishing the necessary skills and a certain routine for attacking identified vulnerabilities.

An insurgent struggle against militarism

Identifying vulnerabilities is certainly a step in the right direction. Mapping the "defense industrial base" with an eye to its vulnerabilities is an enormous and long-term project that anarchists in the U.S. have barely begun. An initiative in the German context could provide inspiration: *"Attack the Arms Industry."* It collects companies and institutions into the categories of producers, suppliers, logistics, research, financing, and legitimization. They have written a tutorial sharing their approach entitled *"An Introduction to Mapping the Local Arms Industry and its Vulnerable Points."*⁸ As in the '60s, disillusioned soldiers and veterans are well positioned to undermine the military with their access to insider knowledge, and this information would be easier for them to share anonymously if an equivalent project existed for the U.S. context.

⁷ <https://ruestungsindustrie.noblogs.org/>

⁸ <https://ruestungsindustrie.noblogs.org/eine-einfuehrung-in-die-kartografierung-lokaler-ruestungsindustrie-und-ihrer-sensiblen-punkte/>

beyond the well-secured perimeter of a factory, decentralized to such an extent that even a militarized police force would be incapable of protecting them.

To return to the proposal in *"Fragments for an Insurgent Struggle..."*, it suggests that an anti-militarist practice could sabotage "the entire logistical system in which these weapons are shipped, loaded, transported by rail or truck, rather than limiting itself to attacks on logistics companies," as well as focusing on "the frequent freight rail connections of weapons companies' production sites."

The "dual-use" infrastructure that serves logistics quickly becomes the infrastructure of war when the State goes to war or has to turn against its own population in an insurgency scenario. The text *"War Starts Here: Let's Cripple its Infrastructure Where We Can"*⁵ criticizes that *"Fragments for an Insurgent Struggle..."* leaves out "the most important raw material of war: oil or energy in general. Especially at the beginning of a war, the amount of energy needed to move troops is gigantic, but throughout the war, fuel has to be transported from some stockpile and/or refinery to the front, where it is needed to fuel the engines of the war machines. And especially when a war is not taking place directly in their own territory, but the logistics of supplying the troops with energy pass through this territory, it might be worthwhile to take a closer look at this infrastructure."

In a very inspiring recent initiative, comrades did exactly that⁶ in the context of the EU's

The world's largest defense contractor, Lockheed Martin, saw its annual revenue drop by 8.9% between 2021 and 2022 due to supply chain constraints (in other words, it couldn't produce \$6 billion worth of weapons). Of the 41 other U.S. companies in the "Top 100," 31 also saw their annual revenue decline for the same reason. By identifying the specific supply chain bottlenecks that are already severely hampering these leviathanic entities, it becomes possible to exacerbate shortages in a way that *actually impacts* weapons production.

Supply chains consist of "tiers" and look more like a network than a linear "chain." First tier suppliers directly supply a company like Lockheed Martin, second tier suppliers supply the first tier, and so on. The average U.S. aerospace company relies on about 200 first-tier suppliers, and the second and third tiers involve more than 12,000 companies. Irreplaceable suppliers are called "sole-source," and are often present at all tiers. As one engineer recently warned in the trade press, "Dassault has five thousand suppliers for its Rafale, and all it takes to block everything is for one to get stuck."

In addition to supplying product components, supply chains must also provide specialized factory machinery. For example, the production of the machinery required for the microelectronics (semiconductors) used in virtually all military technology is a severe bottleneck causing shortages in this sector. In February 2022, the Department of Defense (DoD) released an action plan for *"Securing Defense-Critical Supply Chains"* which warns that "the high-tech company ASML (Netherlands) is currently the sole-source for extreme ultraviolet (EUV) lithography tools that are required to mass produce semiconductor die in technology nodes below 7nm1.³ Such consolidation

5 <https://actforfree.noblogs.org/2022/04/10/publication-war-against-war/>

6 <https://actforfree.noblogs.org/2023/12/19/ten-t-military-logistics-and-availability-using-the-scan-med-corridor-and-its-current-sub-projects-as-an-example/>

3 Microelectronics products containing silicon die chips are typically described as being manufactured at a certain

increases sole-source risk in the global microelectronics supply chain." ASML produces only about 40 machines per year (each taking 12-18 months and involving more than 1,000 first-tier suppliers). They have a \$50 billion backlog and their closest competitors are a decade behind EUV technology.⁴

All supply chains have bottlenecks, and most have "single points of failure," it's just a matter of locating them. The tools to gain this visibility are included in the field of "supply chain risk management"—our enemies are publishing much of this research. The same DoD action plan describes "persistent sub-tier2 supply chain vulnerabilities, from raw materials and chemical shortages to critical subcomponents produced by fragile suppliers." It goes on to provide a high-level overview of supply chain issues for "areas in which critical vulnerabilities pose the most pressing threat": missiles, batteries, castings, microelectronics, and critical minerals.

More recently, for the first time in its history, the DoD released a "*National Defense Industrial Strategy*" to provide a roadmap for "developing more resilient and innovative supply chains." Their

technology node (e.g., 45 nanometers), which refers to the dimension in nm of the smallest element in a transistor. State-of-the-Art (SOTA) is currently considered to be <10nm and is used in advanced computing (data centers, artificial intelligence, supercomputers, etc.). State-of-the-Practice (SOTP) is between 10nm-90nm and is generally what is used in conventional weapons, although today's SOTA will become SOTP and legacy in the future. The industry needs ASML's EUV technology to keep Moore's Law alive ("the number of transistors on microchips doubles every 2 years"), which is necessary for computing to progress. The DoD action plan goes on to say that "although most of DoD's current systems are reliant on State-of-the-Practice (SOTP) and legacy microelectronics, State-of-the-Art (SOTA) microelectronics are DoD's primary differentiator for asymmetric technology advantage over potential adversaries."

4 <https://actforfree.noblogs.org/2022/09/02/asml-semiconductor-dependency/>

plans are not infallible—one advisor describes the document as lacking "a focus on long-term solutions to supply chain issues that have plagued the defense industry." Equally interesting are the publications of RAND's National Security Research Division, especially those of its National Security Supply Chain Institute.

The infrastructure of peace is the infrastructure of war

Logistics means the movement and storage of goods between different points in the supply chain (e.g., from manufacturing plants to assembly plants to distribution centers). Logistics works through infrastructure. Not all supply chain problems involve logistics—for example, a supplier's factory burning down has nothing to do with whether the component can be moved efficiently, but rather whether it can be produced.

The angles of attack can be adapted to the context: a supply vulnerability depends on *supplier bottlenecks*, and a logistics vulnerability depends on *infrastructure bottlenecks*. For example, an arms factory may be located in a region with ample infrastructural redundancy that would make sabotaging logistics difficult, but perhaps it has a sole-source supplier. Conversely, the factory may have invested in building a supply chain with significant redundancy, but its product is shipped to market through ports with limited rail connections.

Regardless of supply and logistics flows (which, it must be emphasized, are generally fraught with severe bottlenecks), a factory needs to be connected to a functioning electrical grid in order to operate, and it often needs to be connected to the Internet via fiber optic cables. Energy and telecommunications vulnerabilities extend far