FERNDON

ARE YOU ON THE LIST?

A INTELLIGENCE TARGETER'S PERSPECTIVE:

HOW 2ND AND 3RD TIER DEFENSE INDUSTRIAL BASE (DIB) MANUFACTURERS ARE IDEAL TARGETS FOR FOREIGN ATTACK

Authors: Dawn Hersey, Ph.D.
Robert Ravert
Cutoff: 20 August 2026
Contact: Team@Ferndon.com
URL: https://ferndon.com

Are you on the list?

A Intelligence Targeter's Perspective: How 2nd and 3rd Tier Defense Industrial Base (DIB) manufacturers are ideal targets for foreign attack

Authors: Dawn Hersey, Ph.D.; Robert Ravert

Information Cut-off: 20 August 2026

If a chain is only as strong as its weakest link, and you are a part of the defense supply chain… do you know what constitutes a targetable link for the DIB?

Many 2nd and 3rd tier DIB manufacturers have not internalized the significance of their impact to sustaining the American military might – and how those wishing to impede our national military resilience would prefer a bloodless targeting of our DIB and the ability to arm our military persons versus face us in open combat.

An obvious way of interfering would be to **delay, disrupt, degrade, or limit** the production of American military materiel through **misinformation, disinformation, propaganda, cyber-attacks, general tension, insider threats, and doubt in the system.** For the DIB, it is the 2nd and 3rd tier manufacturers who make the most practical targets with the greatest potential return on targeting investment.

What! How? Why?

The United States of America is an industrial nation, great and vast, with many redundant nodes and overlapping security features. However, any strengths can be made liabilities.

The secondary and tertiary effects of infrastructure failure are determined by the scope and magnitude of the failure. So, bear with me:

If someone seeks to attack the USA, what is the ultimate goal? Revenge, Retribution, Repression? Is there an end goal or simply a desire for mayhem? Attacking outright generates a response – a unification against the known threat. To undermine, sow the seeds of discord through dividing a nation. Historically speaking, an outsider does not make a difference to the internal machinations of a sovereign nation. Usually, any catastrophic event from the outside unifies a nation unless the nation is already depressed or oppressed (recall America on 12 September 2001). But mayhem can be caused by non-attributable means now: think of misinformation, disinformation, propaganda, cyber-attacks, and just the general tension surrounding political discussions.

For each prospective target, a skilled planner seeks to answer the following questions:

1. **How many customers are affected?** What is the scope of the failure?
2. **What primary resources are affected?** Primary resources such as power plants, substations and end users.
3. **What are the likely secondary and tertiary impacts?** Does power grid failure affect the communications lines? Waterways, watershed areas, water supplies, pumping stations or reservoirs? Railways, commuter or commercial?
4. **What level of severity do I need to bring about my desired intent?** Can the failure be simply a delaying annoyance or must it be catastrophic destruction? There are multiple impacts: Disrupt, Destroy, Delay, Degrade, Deny, or Limit.
5. **Do I want them to know it was me?** Attributable attacks and outright destruction draw focus and attention. If my intention is to undermine them or impede their military, I likely do not want to incur a direct military response. Attributable attacks are generally done by those already engaged in conflict or someone trying to pick a fight.

Now, let us take this one step further. Consider a notional situation where America's military presence is a liability for another state's desired expansion.

For this example, let us look at China's interest in Taiwan and the South China Sea with dates projected as early as 2027. Chinese naval strength has been growing and is considered a

dominant force in the Western Pacific. The contended areas are generally islands, and troops, materiel, and effective controlling resources would need to be transported over large bodies of water. Such a movement would be challenging to disguise and would be likely pre-empted by control of the shipping lanes.

Chinese doctrine

Chinese national objectives can be broken into two primary categories: security and development. These categories are entwined in that security necessitates resources; resources enable development; development builds security. This stretches into regional development and stability. China is not just focused on internal development but sees the ability to control resources and the surrounding region as key to its development and stability.

The Chinese National Intelligence Law, passed in 2017, mandates that **ALL Chinese persons and organizations must assist with intelligence collection.** This includes all Chinese students, Chinese companies, and Chinese professionals. This mandate supersedes any other legal requirement, non-disclosure agreement with an employer, or commitment for confidentiality. These entities may be required to collect information on people, steal information from research laboratories or companies, install backdoors into systems for future collection, or any other myriad of tasks to enable greater Chinese intelligence access. They must also adhere to absolute confidentiality regarding their support of Chinese Intelligence collection.

Chinese Military Tactics are similar but dissimilar to that with which we are familiar. China sees conflict along a continuum that ranges from deterrence to outright combat. The deterrence aspect emphasizes optimal placement of military resources both to deter and also enable maximum impact. This includes but is not limited to placement of military equipment, spies/saboteurs, cyber backdoors, technical vulnerabilities, listening systems, logistical nodes, and more. China includes the ideas of cyberwarfare as part of what Americans translate as "Information Operations." However, Chinese "Information Operations" or *xinxi zuozhan* (

信息作战) emphasize information warfare, concealment, deception, and trickery; the actual execution of this concept, in Chinese *xinxi zhan* (信息战), refers to direct, specific offensive and defensive actions such as Electronic Warfare and Cyber Warfare.

When shifting from "shaping" operations that emphasize spying, sabotage, subterfuge, and resource control, the Chinese emphasize "all-domain" warfare. Chinese military prioritizes advanced technologies to achieve decisive successes through exploiting vulnerabilities in the enemy systems through precise strikes at key points across services and domains. They prioritize nodes in communications infrastructure, energy systems, decision making, and key logistical supply and distribution networks. Further, they see civilian and military entwined as all parts of the same network. ***America's civilian manufacturers are not immune to a military attack.***

What does this mean to 2nd and 3rd tier manufacturers in the DIB?

For one example, consider the Chinese approach to constraining America's ability to project forces and limit our ability to defend Taiwan. One primary method of attack (and defense) in a Chinese scenario would focus on missiles and attack drones. America's ability to respond to a Chinese military action is a key consideration. Current stocks, produce-ability, and re-supply of key missile systems and attack drones would be of direct consideration to the Chinese planners.

If China wanted to execute a military take-over to which America is opposed, it would be of value to mitigate the production of more missiles. If America is likely to have insufficient supplies to easily stop a fully mobilized and intentionally focused Chinese force, then the Americans are less likely to interfere. Resistance to Chinese aggression would be weaker. Dominance with minimal bloodshed is preferred.

If an opponent wishes to minimize the likelihood of American intervention, it is in their interests to minimize reproduction capacity of key military assets. Make intervention a clear liability.

How to delay, disrupt, degrade, or limit the production of American missiles.

How would one do that?

Attacking the military supply itself is counter-productive: the action is overt, the intent clear, and the attack likely attributable (and, as such, inclined to induce an unappreciated response).

Attacking the prime contractor also has a less than ideal return on investment: most prime contractors have a lot of funding to throw into security, and they're very focused on maintaining their contracts and standing. They would fight ferociously using any means available. And they're expecting it.

But, to delay, disrupt, degrade, or limit – does one need to hit the final product? Or could they find a single mineral that is required and block its import? Or find a specific producer of a key component – and sabotage that component 10 steps down the supply chain. Or infiltrate a lab and install a backdoor to gain access to codes for one small part of another component that enables automatic control of that one piece and or the ability to sabotage the project.

And who will know what was done, when it was done, or who even really did it?

A non-attributable sabotage will reduce the likelihood of American diplomatic, economic, or military response while simultaneously undermining America's capacity to project force overseas and defend its interests.

What systems of interest justify a potential target to reduce American Military's ability to operate with confidence?

Let's look at the Patriot missiles, THAAD Interceptors, and the Reaper Drones:

According to the Center for Strategic and International Studies (CSIS), the number of Patriot interceptors fell from 2,330 before the war to 1,030 when the April ceasefire took effect. Following recent fighting, the stockpile is now estimated to be between 759 and 827, a decrease of at least 65% since before the conflict began.

CSIS also estimated that the number of THAAD interceptors fell from 452 before the war to between 232 and 262 at the start of the April ceasefire. Even though the US was able to

replenish some of the inventory to between 234 and 278 interceptors, the stockpile was still assessed at least 38% smaller than it was before the conflict.

And, a favorite legacy OEF/OIF drone: the Reaper. Apparently, Iran has shot down ¼ of our reapers. (Washington Post)

Under the current delivery projections noted by CISI, **Land Attack Missile (TLAM)**, **Terminal High Altitude Area Defense (THAAD)**, and **Patriot Missiles**, which have seen heavy use in the Persian Gulf, are expected to take upwards of 3 years to replenish to pre-2026 levels. **And those reapers?** Those will likely take just as long.

Even if the USA ramps up production, it could take a year to make a significant dent in that re-supply.

This means that a great time to strike or act with minimal likelihood of significant intervention would be between now and when industry is able to ramp up to war production footing. The last time the USA ramped up to war production footing with a strong economic emphasis on providing necessary military equipment and resources was WWII, and that took a few years. Even expedited, it is likely to not be able to restock these missiles to sufficient levels for a significant engagement with a non-depleted military like China's within 6 months.

This puts a threat actor's "action" window out 6-10 months from the publications associated with missile stock depletions and emphasis on ramp-up (July/August 2026). To extend this window past 6 months can be done by impeding production and undermining the American Industrial Machine.

For China, a 6-month window is too short. The weather impacts operations, and prime times to invade Taiwan are in March/April. A 6-month window takes us to January/February of 2027 during the Chinese New Year. Winter of 2026-2027 has an El Niño that is projected to bring excessive heat and rain. Why does the weather impact my planning? Planned military action –

and shipments of produced semi-conductors – are likely to be delayed until March/April. This further means that there will likely be a buildup of supply in Taiwan moving during March/April 2027 as shipping opens back up. Chinese control over Taiwan during this time period would be more conducive with weather and, also, potentially yield the result of winter's microchip production. Extending the "action window" and moderating the American ability to produce quality in a rapid fashion would align with both Chinese doctrine and the situation.

How can an opponent extend their window?

While there are more ways to impede military response, this short article will look solely at extending the window. A targeter asks: What specific vulnerable points can be impacted to impede this restocking timeline and give my planners a larger window?

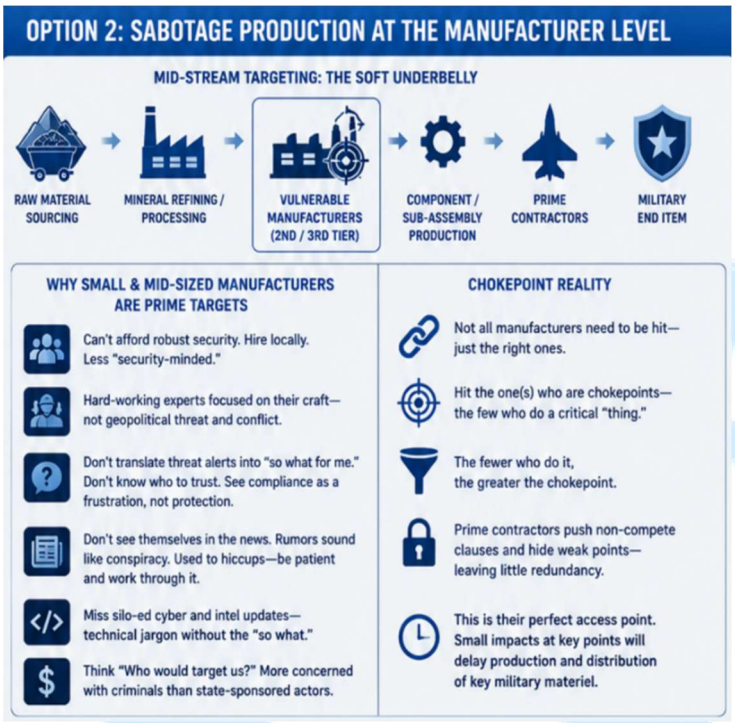
OPTION 1: Can I control the export or trading of a required mineral?

China has a strong and very pertinent impact on Myanmar, Malaysia, Vietnam, and Cambodia, to name a few. They are the regional hegemon and are actively influential of these countries' governments.

BRICS is a strong economic trading coalition of Brazil, Russia, India, China, South Africa, Egypt, Ethiopia, Indonesia, Iran, and the United Arab Emirates. So, if Ethiopia, Indonesia, Brazil, or another of these countries is a point of origin, there is a stronger tie to other members than to the USA.

We are already seeing many sourcing states in the South Pacific, especially, *diversifying their portfolio and building an alternative-to-American market for their goods*. We have also seen, too, that *Chinese companies and entities are actively seeking to control the market for certain elements and minerals – and the ports that export those resources*. And we know, finally, that *supply and demand are intrinsically linked*: what is the likelihood that costs for resources will skyrocket as soon as the market is more directly controlled?

If the prices climb exponentially and reserves become depleted, can a manufacturer afford a significant price increase on resources for a contract to which they already committed? What are the ramifications if they cannot?



OPTION 2: Can I sabotage their production at the manufacturer level?

This would be a "mid-stream" targeting – if the sourcing is out of control or too late for an immediate or timely return on targeting investment, where can one impact between the sourcing and the final production? This is also more likely to have the desired impact of a *delay* in the desired time frame because one cannot account for all the reserves, innovative changes, and possible surges of resources to gain the rare elements.

The military and large prime contractors are hard targets. Who can't afford robust security, hires those they can afford or who work locally, and is less likely to be "security" minded?

The hard-working smaller manufacturers. The ones where the leadership grew up in the business: those diligent laborers who work long hours, build rapport with their colleagues, and who are experts in their field.

This is a **different world from geopolitical threat and conflict**. The languages are different; the foundational knowledge is different; the responses are different.

In this world of smaller and mid-sized manufacturers, many leaders don't translate those "threat alerts" from random analysts or government agencies into "so what for me" (if they even see them). They don't know people in the intelligence industry who can say "this is what's likely coming at this time that pertains to you". Many don't trust the government or other "consultants" digging around in their business. They see their compliance checklists as a frustration and those enforcing them or explaining how to implement them as talking heads or good idea fairies.

They don't see an alert that they'll be attacked in the news – and a lot of the rumors of attacks sound more like conspiracy theories. They're accustomed to hiccups or problems – be patient and work through it. They don't hear all the updates on siloed hacker or intelligence chats (even if they did, it's discussed in technical jargon without the "so what" for them). Who'd want to target a small manufacturer: they're not super wealthy. They are concerned with criminal

behavior more than international threat from a highly skilled and focused targeter looking for an accessible node in a greater supply chain.

Not all of the manufacturers need to be hit: just the right ones. Just the one(s) who are a chokepoint on the chain. Just the one(s) who create or refine or process that single component. *The fewer who do a particular "thing", the more this "thing" and those companies are a supply chain chokepoint.*

And it is known, too, that prime contractors are greedy and want non-compete clauses with their subcontractors whenever possible. And they don't like admitting when there is a failing point in their chain publicly. They try to work around it fast and hard. Which means that the smaller manufacturers don't always have a lot of redundancy – and they may be dropped for a lesser qualified producer who promises fulfillment. *That drop creates the desired delay for the targeting team while the manufacturer is collateral damage.*

This is their perfect access point. All of these small impacts at key points will *delay* the production and distribution of key military materiel. This extends the action window.

How to impact a small or medium manufacturer.

If these smaller manufacturers' security is good enough to notice the threat, they might think it a "one-off" from a criminal or a "glitch". Quite likely, they may see the problem and not even know it's a threat or that it's an outsider wreaking havoc on their internal systems.

This is where one strikes to hit. There is no need to destroy. **The need is to DELAY**. To slow down final production and distribution.

How would one do this? There are several ways, and here are just a few.

1. **Small Businesses.** Use their small business certifications as means to bracket. Small Businesses and those which are disadvantaged are more likely to be targetable – because they're small and disadvantaged and, in so defining, less likely to have resources to bear on a threat. If they're economically disadvantaged, they are less likely to have the robust network of advanced expertise very helpful when seeking to mitigate and address an unattributable sequence of "glitches". They'll go with who they know and what they can readily afford. Or they will try to just endure it.
2. **Rural or Economically Constrained Locations.** Use their location against them. If they're rural or located in less economically robust communities (like HUB Zones), one can impact their water, sewage, electrical, or other systems with old Operational Technology.

This could create power surges, facility damages (we love sewage backups into facilities), or even water cut-offs or contaminations.

3. **Accessible Systems.** Sabotage their supply through remotely triggering a payment issue or unreliability reports. Reputations can be soured fast – and finances are sensitive for everyone.
4. **Exploitable Technology.** Access their programs and maybe change small parts of the production guidance that could either sabotage overtly or create a triggerable sabotage (like the Israelis' exploding Hezbollah pagers or Stuxnet). If it's not found, awesome. If it is, the entire production line will have to be taken off for evaluations and a possible re-run.
5. **Weather Impacts.** Use weather to disguise and amplify my impact. If this is a northern area, for example, do this in the winter. Especially with a bad storm with heavy snow or ice. If I can trigger the surges in alignment with such a storm, who will know it was me that fried everyone's systems?
6. **Insider Risk.** If this target is sufficiently important, possibly work to have insider access. Payments during times of economic hardship, an invaluable researcher or scientist with family held hostage in China, or even a disgruntled employee: the insider can enable better access to systems, directly enable sabotage, and even help refine attack timing to align with more nuanced contexts (like a leadership divorce or childbirth, internal celebrations, or even security personnel turn-over).

There are so many ways to *delay* production. And it's not all about UAVs or explosions or massive cyber-attacks. It's small and intentional. It's targeted and focused. And, with the foes more likely to desire a delay, it will likely be unattributable and severely damaging to the business health of a smaller manufacturer.

Conclusion

Now I ask to the smaller manufacturers within the Defense Industrial Base – are you good at what you do? Do you have a non-compete clause? Are you located in an economically disadvantaged or rural region? How many competitors do you have? Do you know the final destinations for your components?

You already know your supply chain. Ferndon's question is whether you know who else is looking at it and which seemingly insignificant dependency they would recognize as consequential before you realize its importance.

Are you on the list?