

SECURITY

Security Is Resilience

Real security is the ability to withstand and recover from shocks, not military strength alone. And the adversaries already agree.

PILLAR 10 · DEMOCRATIC SECURITY IN A CHANGING WORLD

AT A GLANCE

The problem

Adversaries prepositioned in civilian infrastructure, 90% of leading-edge chips from one island, and hundreds of drugs in shortage.

The proposal

Security as resilience: hardened essentials, diversified supply, local capacity, exercises that test it all.

Cost & funding

Priced like insurance; far cheaper than the failures it prevents.

Evidence strength

Strong threat documentation (CISA, official records); posture effects are hard to test, so exercises are the evidence engine.

Principal risk

Resilience spending disproportionate to the risks it insures; alliance strain from conditionality.

Success looks like

Exercise performance improving; single-point dependencies falling year over year.

Summary

Security is resilience. A country is safe not only when it can project force but when it can take a punch and keep functioning: when its supply of essentials does not hang on a single point of failure, when its grid and networks can absorb an attack, when it can detect and contain a disease before it becomes a catastrophe, and when its communities can care for themselves through the first hours of a crisis. Here is the part that has changed: our principal adversary now agrees. CISA, the NSA, and the FBI jointly assess that Chinese state-sponsored actors known as Volt Typhoon have pre-positioned inside American water, power, communications, and transportation systems, not to spy, but to be able to disrupt them in a crisis.

This brief proposes seven planks at home: secure the supply chains we cannot live without at the layer where the dependence actually lives, build energy independence and a grid that can take a hit, defend the lifelines and fund the defenders, rebuild biological defense, sustain alliances and defend democratic institutions, treat local resilience as national security, and exercise the whole system. Abroad, three principles: secure our own people first, no unconditional aid and one standard for every ally under the Leahy Law, and force as a last resort, for moral ends, decided in the open.

The Principle

Security is resilience. A country is safe not only when it can project force but when it can take a punch and keep functioning: when its supply of essentials does not hang on a single point of failure, when its grid and networks can absorb an attack, when it can detect and contain a disease before it becomes a catastrophe, when its institutions can resist subversion, and when its communities can care for themselves through the first hours of a crisis. The most secure country is not merely the most heavily armed. It is the most resilient, the hardest to disrupt and the fastest to recover.

Here is the part that has changed since this argument was first made: our principal adversary now agrees with it. The documented posture of Chinese state cyber operations against the United States is not aimed at our military. It is aimed at our lifelines, the water, power, communications, and transportation systems civilians depend on, precisely because disrupting civilian resilience is how you paralyze a modern country without firing a shot. When the other side has reorganized its strategy around attacking your resilience, treating resilience as the core of your defense stops being a reframe. It is just an accurate reading of the battlefield.

The System Failure

We have spent enormous sums on military hardware while underinvesting in the resilience that determines whether people are actually safe, and the evidence of the gap is no longer hypothetical. It is documented, attributed, and sitting inside the walls.

Start with the intrusion. CISA, the NSA, and the FBI jointly assess, with high confidence, that Chinese state-sponsored actors known as Volt Typhoon have compromised the networks of American critical infrastructure organizations across communications, energy, transportation, and water systems, in the continental United States and in Guam. The agencies are explicit that this is not espionage. The pattern is pre-positioning: quiet, long-term persistence inside operational systems, using legitimate administrative tools to avoid detection, so that in a crisis or a conflict the intruder can disrupt the water, the power, and the ports at a time of its choosing. The FBI's director called it the defining threat of our generation. These actors have held footholds for years, they have regained access after being evicted, and a parallel campaign, Salt Typhoon, burrowed into the major telecommunications carriers deeply enough to reach call records and the government's own lawful-intercept systems.

Now notice where they went, because it vindicates this platform's least glamorous argument. One documented Volt Typhoon intrusion sat for nearly a year inside a small municipal light and water department in Massachusetts, mapping how the local grid works. The adversary is not only targeting the marquee systems. It is targeting the small, local, under-defended utilities where the seams are, the exact layer of American infrastructure this platform has argued we starve. And the exposure is compounding: utilities absorbed over eleven hundred cyberattacks in a single recent year, up 75 percent year over year, while the grid's own reliability authority warns that its points of susceptibility grow by roughly sixty a day as digitization outruns defense.¹ Russia showed the world what the end state looks like when it turned off power to hundreds of thousands of Ukrainians in 2015 and 2016. Meanwhile the civilian agency built to defend all of this has been cut, not grown, in the middle of the campaign against it. Weakening your own defender while the intruder is inside the house is not a policy disagreement. It is negligence with a signature on it.

The supply-chain exposure is the same failure in a different domain, and the concentration is stark. Taiwan accounts for more than 60 percent of global foundry revenue and over 90 percent of leading-edge chip manufacturing,² with a single company producing as many wafers a year as the entire United States. Everything advanced in the American economy and military runs through a strait the adversary has publicly committed to crossing. Medicine tells the same story with a subtler twist that honest policy has to respect: America's dependence on China runs deepest not in finished drugs but in the earliest, least-regulated stages of ingredient production, which means onshoring the final pill accomplishes little if the raw materials underneath it are still single-sourced abroad. The pandemic already gave the country a live demonstration of what these dependencies cost when they snap, and drug shortages have stayed severe by historical standards since, peaking at a record 323 active shortages in early 2024 and still running above 200. And beneath all of it sits the brittleness this platform names everywhere: we centralized and globalized the systems people depend on, let local capacity wither, and left too little underneath to catch the fall.

The Proposal

Seven planks at home, three principles abroad.

1. **Secure the supply chains we cannot live without, at the layer where the dependence actually lives.** Identify the essentials the country cannot lose access to, medicine and its raw ingredients, semiconductors, critical minerals, key elements of the food supply, and build secure sources through domestic production and trusted allies, with strategic reserves where they make sense. Follow the dependence to its real depth: for medicine that means the raw materials and early chemistry, not just the finished drug, because onshoring the label while importing the substance is security theater. For chips it means sustaining the domestic fabrication build-out already underway and pairing it with the packaging, materials, and talent that make a fab more than a building. Diversification and trusted sourcing, not autarky.
2. **Build energy independence and a grid that can take a hit.** Treat clean, domestic energy as the security asset it is, and harden the grid against weather, physical attack, and cyber intrusion, with the redundancy and distributed generation that let parts of the system fail without taking down the whole. Energy a country produces itself, on a grid that can absorb a blow, is far harder to hold hostage, and a distributed grid is a harder target than a centralized one by design.
3. **Defend the lifelines, and fund the defenders.** Make the cyber defense of water, power, communications, and transportation a first-order national defense mission, funded like one. That means restoring and growing the civilian cyber defense agency rather than cutting it mid-campaign, mandatory baseline security standards for lifeline utilities with federal help to meet them, because a small municipal water department cannot out-spend a state intelligence service alone, and sustained threat-hunting that treats eviction as a process rather than a press release, since these actors demonstrably come back. Pair defense with consequence: attribution, indictment, and sanction, jointly with allies, so intruding on American lifelines carries a price.

4. **Rebuild biological defense before the next test.** The pandemic was a national-security failure no weapons system could have prevented, and the preparedness it exposed as thin has been allowed to thin further. Fund the disease surveillance, public-health workforce, and medical countermeasure capacity to detect and contain outbreaks, natural or engineered, before they become catastrophes, and connect it to the public-health infrastructure the foundations pillar rebuilds. Biological threats are among the most likely and most dangerous the country faces, and among the most neglected relative to their risk.
5. **Sustain alliances and defend democratic institutions as security assets.** Alliances multiply national strength, and the integrity of elections and public trust is a security perimeter in its own right, under documented attack from foreign interference and domestic subversion alike. Defend both, within the law and with full respect for civil liberties, because security measures that erode the freedoms they protect defeat their own purpose.
6. **Treat local resilience as national security, because the adversary already does.** A country whose communities can absorb shocks locally is fundamentally harder to destabilize, and the intrusion record shows the adversary probing exactly that local layer. Invest in it as defense: local emergency and public-health capacity, distributed energy and microgrids, local food systems, and the community institutions and mutual-aid networks that do the first work in any crisis. The resilience lives locally. The financing, standards, and coordination that get it to scale are the federal job.
7. **Exercise the whole system.** In emergency management, a plan that has never been exercised is a rumor. Run national-scale exercises that stress the seams these threats actually target, a grid-down week, a port disruption, a supply-chain snap, an outbreak, with states, localities, utilities, and communities in the room, and fix what the exercises find. The cheapest disaster is the one we prevent, and the second cheapest is the one we rehearsed.

Allies, Aid, and the Use of Force

Security is also how the country carries its weight in the world, and that requires a consistent posture rather than improvisation. Three principles govern it.

Secure our own people first. On an airplane you secure your own oxygen mask before helping the person next to you, and the same logic applies to a country. There is nothing wrong with helping our neighbors, and a strong America should. But we should not fund abroad what we refuse to fund at home, and foreign commitments should be weighed honestly against unmet needs here. Helping our own people is not isolationism. It is the foundation that makes a credible role abroad possible.

No unconditional aid, and one standard for every ally. Aid and support come with clear, consistent expectations. Not micromanagement of every operational decision, but a firm line: when a partner uses American weapons and resources to commit atrocities or target civilians, we stop, and the rule applies to every ally without exception. This is not a new idea but an old law we fail to enforce. The Leahy Law already bars assistance to foreign units credibly implicated in gross human-rights violations³, and it has been applied unevenly, with documented double standards for favored partners.⁴ Enforce it consistently, for everyone, because a standard that bends for friends is not a standard at all.

Force as a last resort, for moral ends, decided in the open. As the strongest military power in the world, the United States can sometimes be the difference between a massacre stopped and a massacre completed, and it should be willing to stand against the gravest crimes: genocide, ethnic cleansing, mass atrocity. That is the core of the Responsibility to Protect, grounded in the older just-war tradition. But the bar stays high and the rules strict: authorized democratically, not launched on one person's say-so; specific objectives and a defined horizon, not open-ended occupation; and the people being helped taking part in their own liberation, with America providing support, training, and protection rather than fighting in their place. We should be willing to stand against slaughter. We should never again drift into open-ended wars without clear ends, public consent, or a moral purpose that survives daylight.

Harden the Systems That Keep People Alive

The Volt Typhoon finding earlier in this brief has an unfinished implication: adversaries prepositioned in civilian infrastructure attack water systems, hospitals, and utilities that mostly cannot defend themselves. The position: enforceable minimum cybersecurity standards for lifeline sectors, water, healthcare, energy, with federal technical and financial support for the thousands of small utilities that cannot hire a security team, a ransomware doctrine that pairs disruption of the criminal ecosystem with mandatory incident reporting, and cyber exercises folded into the resilience-exercise regime this brief already proposes. Resilience-first security means the water treatment plant, not just the aircraft carrier.

Implementation Pathway

Supply-chain security runs through industrial policy, procurement, and coordination with allies, much of it begun and in need of follow-through that reaches the raw-material layer. Grid and energy resilience connect to the climate and build pillars through deployment, permitting, and standards. Lifeline cyber defense runs through the civilian cyber agency's budget and authorities, through utility regulation at the state level, and through the federal standards and assistance that make small-utility defense possible. Biodefense runs through the public-health appropriations the foundations pillar carries. The Leahy enforcement commitment is executive-branch discipline under existing law, which is exactly why it is a test of seriousness: it requires no new statute, only the will to apply the one we have. The exercise regime runs through the emergency-management machinery the country already owns. The pattern throughout is the platform's standard one: national coordination and financing supporting capacity that is often built and held locally.

Funding and Public-Value Logic

Resilience is cheaper than catastrophe, and this pillar's spending mostly does double duty. Clean energy lowers bills every day and hardens the country against coercion. Public-health capacity serves people in ordinary times and is the difference between an outbreak and a catastrophe. Local resilience investment pays out in every disaster, attack or storm alike, which is the quiet advantage of defending by resilience: the same dollar defends against the hurricane and the intrusion, because both are answered by communities and systems that can absorb a shock. Securing supply chains for essentials costs far less than losing access to them in a crisis, as the pandemic priced out in real time. And enforcing the Leahy Law costs nothing at all. It saves money, and something worth more than money.

Risks and Guardrails

Reframing security as resilience is not retreat, and the alliance commitments exist precisely to say so; trusted partners are part of resilience, not an alternative to it. Supply-chain security means diversification, not autarky, because making everything at home is neither possible nor wise, and the honest nuance stays in: onshoring that ignores the raw-material layer is theater. Cyber standards for small utilities must arrive with federal money and help, or they become an unfunded mandate that closes the local water department instead of defending it. The defense of democratic institutions stays inside the rule of law and civil liberties, because a security state that eats the freedoms it guards has lost the war by winning it. And the use-of-force principles are guardrails on ourselves: the memory of open-ended wars is exactly why the bar is written high, in public, in advance.

Metrics for Success

Judge the agenda on dependence, hardness, and recovery.

- Dependence on single or untrusted sources for critical goods, tracked at the true depth of the chain, raw ingredients and materials included, and the adequacy of strategic reserves.
 - Lifeline-sector intrusions detected, dwell time, and re-intrusion rates, alongside the funding and staffing of the civilian cyber defense mission.
 - Grid reliability and resilience to weather, physical, and cyber threats, and the share of distributed and domestic generation.
 - Public-health readiness: detection speed, surge capacity, and countermeasure stockpiles, exercised and scored.
 - Leahy Law enforcement applied uniformly, measured by its exceptions, which should be zero.
 - Local resilience capacity in place, and recovery time after real shocks and national exercises alike.
-

Opposition and Responses

Some will say this weakens national defense by looking past military strength. It completes military strength. The documented adversary strategy is to paralyze America's civilian lifelines in a crisis, precisely to blunt its military response. A powerful force sitting on a fragile grid, intruded utilities, and snapped supply chains is not secure, and the joint assessment of our own security agencies says the enemy is already inside those systems. Closing that gap is defense.

Some will say securing supply chains is protectionism. The aim is not to wall the country off but to ensure it is not dependent on a single distant or untrusted supplier for things it cannot do without, through domestic production and trusted allies together. Ninety percent of leading-edge chips crossing one strait is not a market outcome to defend. It is a single point of failure to fix.

Some will say conditioning aid abandons our allies. Enforcing an existing American law, evenly, is not abandonment. It is the difference between an alliance and a blank check, and allies who do not commit atrocities with American weapons have nothing to fear from it.

Some will say the intervention principles tie America's hands. They tie America's hands against exactly one thing: drifting into open-ended wars without public consent or clear ends, which is the failure mode of the last quarter century. A high bar, set democratically, makes the credible threat of action stronger, not weaker, because it is believed.

Some will say local resilience is not national security. The adversary's own targeting says otherwise. When a foreign intelligence service spends a year inside a small-town water utility mapping the grid, the local layer has been designated a battlefield by the other side. Defending it is not sentiment. It is meeting the attack where it is aimed.

What Would Change Our Position

Resilience-first is a testable doctrine. If exercises and real shocks showed the locally-anchored model failing where centralized response succeeded, the balance shifts back toward federal capacity, and honestly. If supply-chain diversification produced costs wildly out of proportion to the risk it insures against, the pace changes. If conditioning security assistance on conduct demonstrably weakened alliances without improving conduct, the tool would be reweighed against the alternatives. The commitment is that security decisions get made on evidence about what actually protects people, not on which posture performs strength best.

Public-Facing Language

Here is the short version. Security is not just about how big our military is. It is about whether we can take a hit and keep going, and our adversaries have already figured that out: they are inside our water systems and our grid right now, not to spy, but to be able to turn things off if a crisis comes. So defend the lifelines and fund the defenders. Secure the supplies we cannot live without, down to the raw ingredients, because 90 percent of the world's advanced chips coming from one island is a single point of failure with a flag on it. Build energy we control on a grid that can take a punch. Get ready for the next outbreak before it arrives. Hold every ally to one standard, the one already written in our law. Use force only as a last resort, for moral ends, decided in the open. And invest in communities that can look after themselves when the worst happens, because that is exactly the layer the other side is probing. Security is resilience. The cheapest disaster is the one we prevent.

SOURCES

1. E&E News (POLITICO) reporting NERC's count of grid susceptibility points growing ~60/day ↩
2. U.S. International Trade Administration, Taiwan country commercial guide: semiconductors ↩
3. State Department, the Leahy Law ↩
4. Human Rights First on uneven Leahy Law application (advocacy source, flagged) ↩