The decentralized approach in the United States for resilience in critical infrastructures may contribute to an uneven and fractured cyber and physical security landscape across states and regions.

The landscape has many fault lines that may become increasingly fragile and vulnerable as technological advances improve, enhancing adversarial targeting capabilities and outpacing governance efforts.

FAULT LINES IN U.S. CRITICAL INFRASTRUCTURE LANDSCAPE

John Rodman, Strategy Futures Reimagined, LLC

The United States Does Not Have a National Resilience Baseline

We have opted for a critical infrastructure model that relies on broad federal guidance and state-determined implementation for protection and resilience of key sectors in our society.

Current resilience is retrospective! It is based on after-action reports, lessons learned repositories, and recommended corrective actions.

There is no unified measure of:

- Infrastructure system robustness
- Cross-sector interdependencies
- State-level readiness
- Private-sector resilience
- National-level systemic risk

The decentralized, state-driven model works reasonably well for hurricanes, wildfires, and floods, if properly financed and managed, but becomes fragile when facing:

- Coordinated cyberattacks
- Multi-vector disruptions
- Cross-border infrastructure targeting
- Adversaries who understand interdependencies better than we do

Natural disasters don't exploit the fault lines. Adversaries do.

Past Requirements for a National Methodology (wave-top)

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (2003) require a uniform methodology and a comprehensive data base. The National Critical Infrastructure Prioritization Program (NCIPP) was created by DHS to fulfill a 9/11 mandate. As recently as 2022, critical infrastructure stakeholders noted in a government report that the NCIPP was of little use. National Security Memorandum 22 required the Director of the Cybersecurity and Infrastructure Agency (CISA) to identify Systemically Important Entities (SIE) but delegated the task to multiple agencies and non-federal entities. Multiple government reports have identified problems with data collection, methodology, and consequence thresholds for singular and connected (cascading) events when working with DHS.

Executive Order 14239 shifts increasing resilience to state, local, and private entities which could lead to less information sharing at that level, a diminished understanding of risk, and an overall reduction in resilience.

U.S. critical infrastructure management is optimized for natural disasters, federal after-action reports, assessments, and budget planning. Federal efforts are not optimized against a systemic adversarial attack or cross-sector infrastructure resilience.

Systemic Risk from Committed Adversaries

The U.S. system for national resilience and vulnerability is built on coordination and not mandated requirements to state and private industry. It also does not include contingency planning for command authority during crisis for even the most important "lifeline" sectors monitored by FEMA*. The current U.S. creates a very large attack surface across our national infrastructure that can be exploited and targeted.

A sophisticated adversary may attack randomly to create chaos or fear, but they may also attack strategically from their committed efforts to:

- Study interdependencies
- Identify uneven state-level protections
- Exploit the weakest link
- Create cascading failures
- Time attacks to maximize political or resource strain

The decentralized U.S. system allows sophisticated adversaries to:

- Hit a state with weaker cyber controls
- Target a privately owned facility with minimal oversight
- Exploit both sector, state, and regional inconsistencies
- Trigger federal response delays
- Create confusion in reporting and prioritization

*Federal Emergency Management Agency

Adversarial data exploitation and targeting requires we move beyond reporting requirements for disaster relief and situational awareness to common federal risk baselines, contingency planning, and oversight of critical and vulnerable sectors.

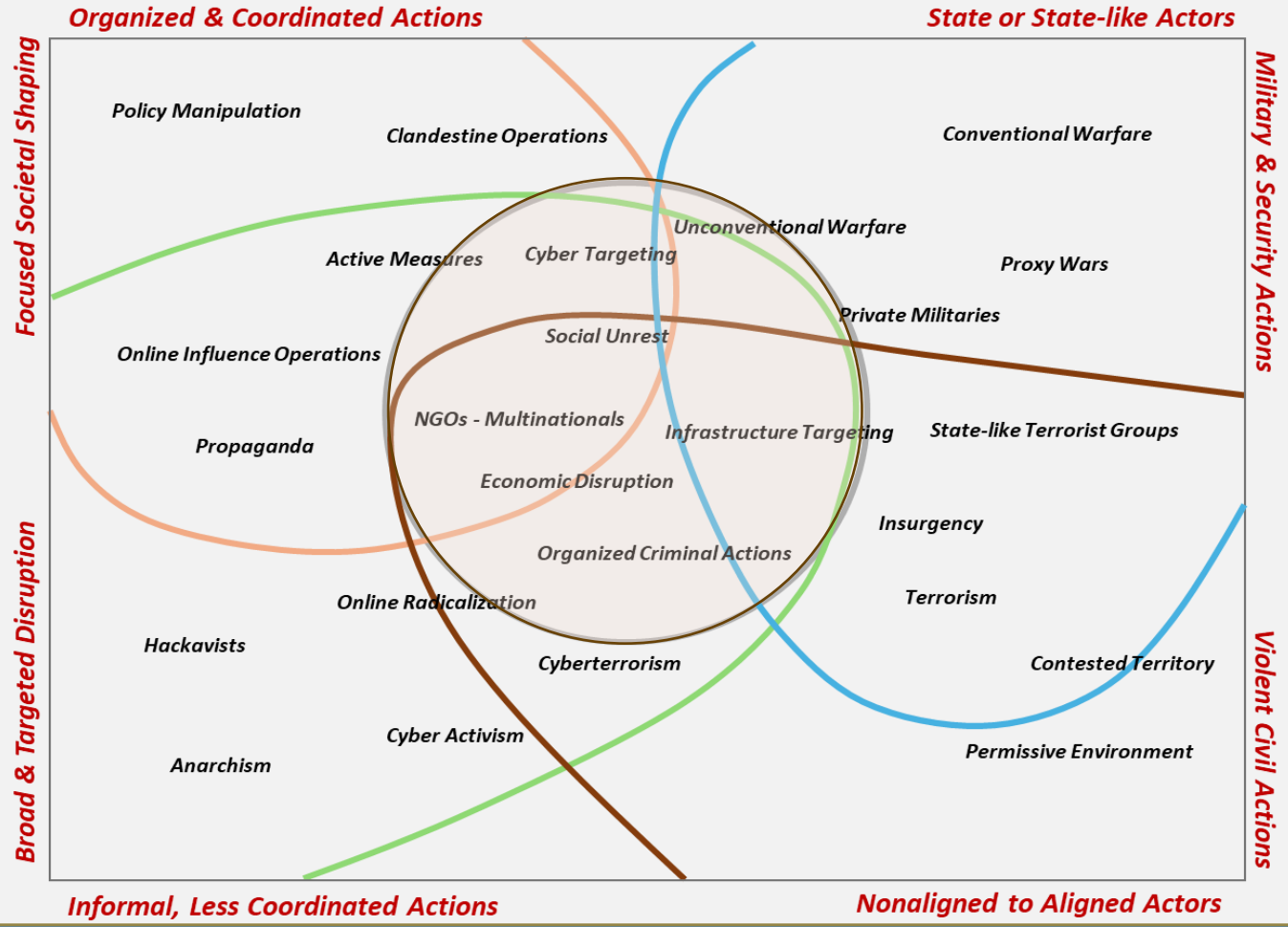
U.S. Decentralization is a Vulnerability in Asymmetric Warfare

A wide variety of actors and actions exist in the asymmetric warfare landscape. For the U.S., the most vulnerable area is the middle where multiple agencies and organizations have overlapping national responsibilities and state responsibilities are uneven or conflicting.*

Mission Sets

- Civil/Law Enforcement
- Counterintelligence & Intelligence
- Cyber Defense
- Counterinsurgency & Counterterrorism
- Traditional Military/Defense

Differing roles, rules, and playbooks create fragmented resilience capabilities in the central, grey area.



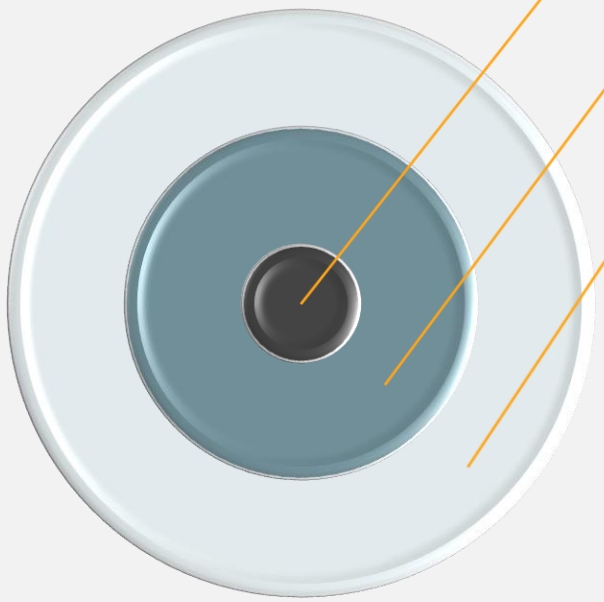
*This graphic was created by the author and is part of a more extensive model on asymmetric warfare.

The lines represent capability "frontiers" and behind them the actions that actors, from sophisticated state to nonaligned violent, may focus or take actions against the U.S.

The vulnerable center zone requires crisis command and control to identify risks and eliminate state-level discontinuity.

Technology Can Amplify Uneven Preparedness and Create Vulnerabilities

States vary widely in their cybersecurity maturity due to differences in IT modernization, implementation of federal guidance, and their reliance on private operators for many of their systems. While technology could connect sectors through common situational awareness; the lack of enforced minimal standards can result in vulnerabilities that weaken the system.



Physical systems at the state and local level often rely on legacy preventative measures and struggle to invest in newer, more advanced technology.

Digital systems integrity, cyber and vendor forensics, cloud and supply chain stability are difficult to maintain and sustain in many states and are unevenly employed despite regionally connected infrastructure.

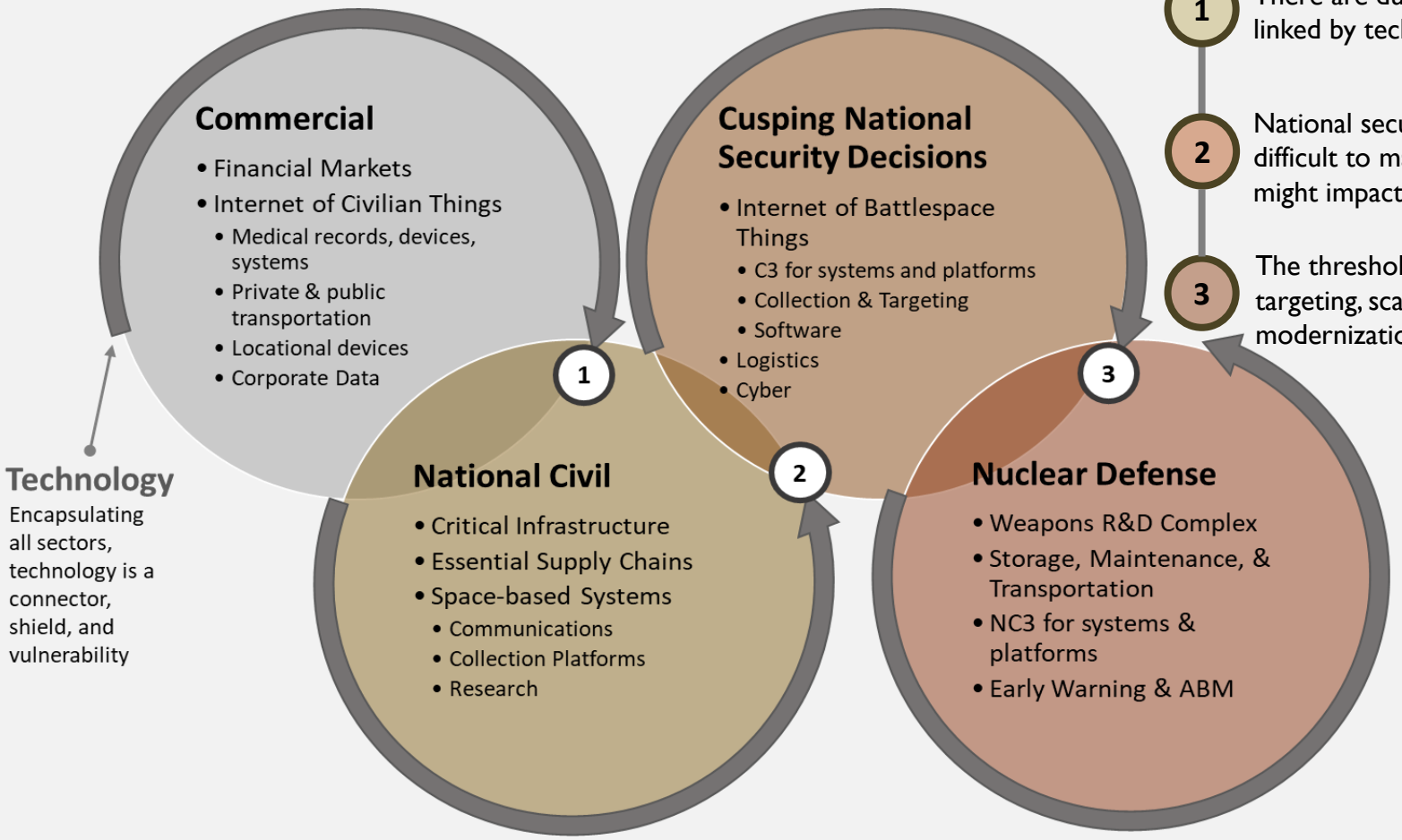
De facto nationally integrated infrastructure in key sectors is occurring without a national governance model, which may create a systems-level vulnerability that may require more federal oversight.

Decentralized resilience limits technology advantage
• Decentralized systems are inherently uneven in application which can create entry points for attackers at the local level that cascade to national levels in a hyper-connected world.
• Many smaller, rural communities are underfunded and lack the skilled workforce to sufficiently employ technology to mitigate risk and increase resilience in local or regional systems.
• Large commercial, private operators adopt technology faster than smaller private operators, and state and local governments may fall further behind.
• Sectors with stronger standards and coordination (like finance or energy) also connect to lesser-protected local civil and production sectors and create opportunities for exploitation.

Creates exploitable weak points (joints) in critical infrastructure system by widening resilience between sectors and their participants and slowing national response in a crisis.

Technology is a creating an unintended centralization, or borderless, level of risk that the current sector lifeline system is ill-prepared for. Interdependence in our critical infrastructure is outpacing federal governance, coordination, and management.

Disconnected Vulnerabilities May Impact National Deterrence*



1. There are dual-purpose or shared aspects of the sectors increasingly linked by technology and dependent vulnerabilities.
2. National security dependency on commercial critical infrastructure is difficult to map and measure. How increasing risk within these sectors might impact national security decisions for critical systems is unclear.
3. The threshold for the use of nuclear weapons may lower due to precision targeting, scaled down weapons, and changing attitudes – leading to modernization on a fragile or fractured critical infrastructure system.

Estimating Dependencies and Mapping Vulnerabilities

1. Vulnerable private systems can overlap with national interests when targeting critical supply chains, infrastructure, or data.
2. National security is increasingly reliant on commercially controlled technology (some overlap of Commercial, National Civil, and Nonnuclear Defense.)
3. Nuclear Defense systems may not interact directly with all the other sectors or have overlapping technology, but there are likely some causal chain effects if other sectors are targeted.

* A partial list of potential vulnerabilities that, if targeted, might cause significant to catastrophic harm to the U.S.

What event in vulnerable U.S. Commercial and National Civil components will impact essential infrastructure or systems to such an extent that it effects national security decisions of safety and use in the nuclear defense and deterrence realm?

John Rodman, Strategy Futures Reimagined, LLC

Comparing Other Nations' Attempts to Reduce Fragmentation and Vulnerability

How other technologically capable nations deal with risk and resilience	Comparison
Infrastructure viewed as a national security asset and not private property	**United Kingdom:** Centralized National Risk Governance
National critical infrastructure strategy encompassing more than broad objectives	**Germany:** Mandatory National Standards, Uniform Execution with Federal Oversight
Federal, cabinet, or parliamentary oversight of cross-sector resilience	**Canada:** Mandated Standards and Frameworks with Formal Provincial Agreements
Mandatory national standards for resilience with penalties for noncompliance	**Singapore:** Fully Integrated and Managed Critical Infrastructure Sectors
Formalized agreements on national and state or provincial responsibilities, including shared	
Data used to create a single national picture of situational awareness available at lower levels	**United States:** Decentralized Authority Over Nonintegrated Cyber and Physical Governance with Voluntary Standards
Ability to identify and test cascading events in multiple sectors	

Local autonomy for protecting critical infrastructure worked when physical systems were not connected to other systems, there were minimal cross-sector dependencies, and adversaries were not able to exploit data to isolate vulnerabilities.

Initial Federal and State Steps to Limit Decentralized Risks

Determining federal policy, the roles of various agencies, and consistent funding for voluntary private entity resilience efforts is further challenged by the problem of scaling methodology and processes to thousands of sector inputs and participants. When National Resilience Strategies are produced, they often offer only broad guidance for nonfederal implementation, no standard or formal methodologies for resilience, and no consequences for noncompliance.*

If a new National Resilience Strategy is created, some basic objectives might include:

	Develop and Implement National Baselines for Resilience in the Meta-sectors	Establish Integrated Rules for Systemically Critical Infrastructure Resilience (SCIR)	Create a Common Situational Awareness Platform to Monitor SCIR in Real-time
Federal Role	• Identify dependencies between sectors and their resilience under various scenarios • Set goals for emergencies that include response, redundancy, and recovery • Ensure there is a stronger connection between planning for cyber and physical resilience	• Designate some infrastructure as systemically important (grids, pipelines, IT, communications backbone, ports, etc.) • Set and impose standards in operation, connectivity, and cyber and physical integration and resilience • Enhance the and expand the use of regional associations and coalitions to implement SCIR requirements on systems connected across U.S. regions	• Leverage current FEMA reporting standards on incidents in a proactive way instead of after-action reporting and remediation • Use standardized data to project forward vulnerabilities in the system with advanced modeling • Reimagine the role of Fusion Centers to combine cyber, physical, and private-sector data into a real-time situational awareness
States	• States must meet baselines and requirements (penalties, fines, withholding of funds) but chose how to meet them	• States agree on shared cross-border lifelines and priorities for protection and restoration through the Board of Governors, possibly a sub-committee	• States provide data in standardized formats, meet minimal baseline requirements, expand their role as first line of defense.

*CISA was very successful in building partnerships, providing advisors, and increasing information sharing, but efforts to get it more authorities and budget for helping states bolster infrastructure often failed. The author advocates for a stronger federal role to create a common operational picture.

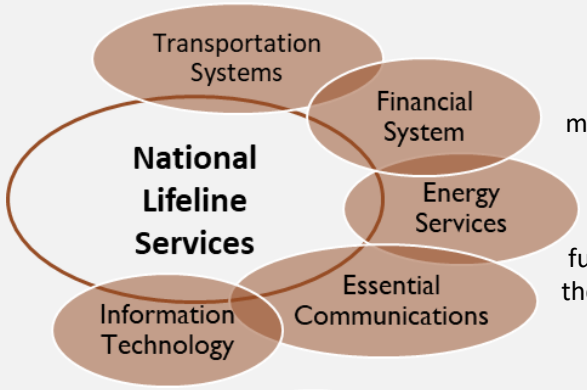
The U.S. has tried for two decades to establish data, methodologies, and requirements for Systemically Critical Infrastructure Resilience. Advances in data and technology can create a Common Operational Picture if properly resourced.

John Rodman, Strategy Futures Reimagined, LLC

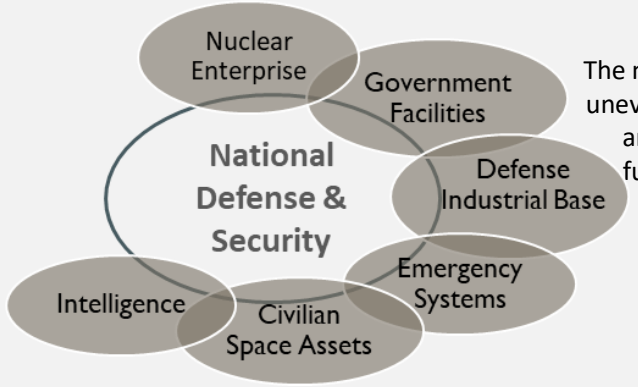
Shifting to a National Lifeline Sector with Aligned Meta-sectors

Critical National Functions

Existing critical infrastructure sectors are realigned below into Meta-sectors that include some new individual sectors added by the author. This realignment is helpful for understanding how Meta-sectors, including an overarching one called National Lifeline Services, can group more specialized sectors into blocs for managing and developing policy/planning. Managing blocs that may have similar needs helps national planners create appropriate governance.

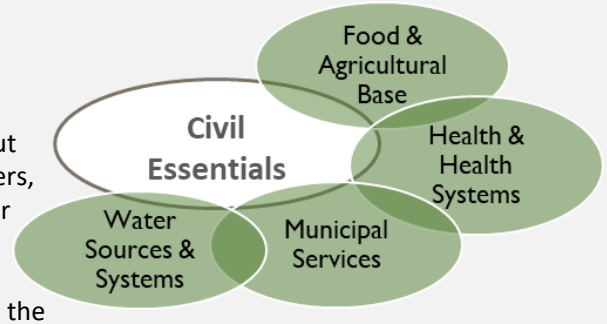


The expanded Lifeline functions bridge and maintain functionality between Meta-sectors – Civil Essentials, Economy & Industry, and National Defense & Security. The National Lifeline services identified in 2013 were functions representing interdependence, but their precise dependencies are not identified, planned for, or aligned.

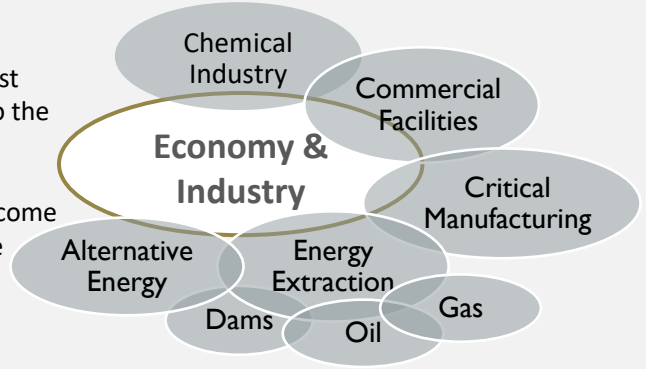


The national defense Meta-sector is an uneven landscape of authorities, roles, and responsibilities for most critical functions but less so for others, like the nuclear enterprise. This will require extensive unwinding of existing authorities of other government entities

Much work occurred during COVID on resilience in health & health systems, but the costs of the pandemic, loss of workers, and adjustments to operations left other sectors vulnerable. We saw this with municipal services and water systems attacks. Like many of the Meta-sectors, the information systems in the Civil Essentials Meta-sector are highly specialized.



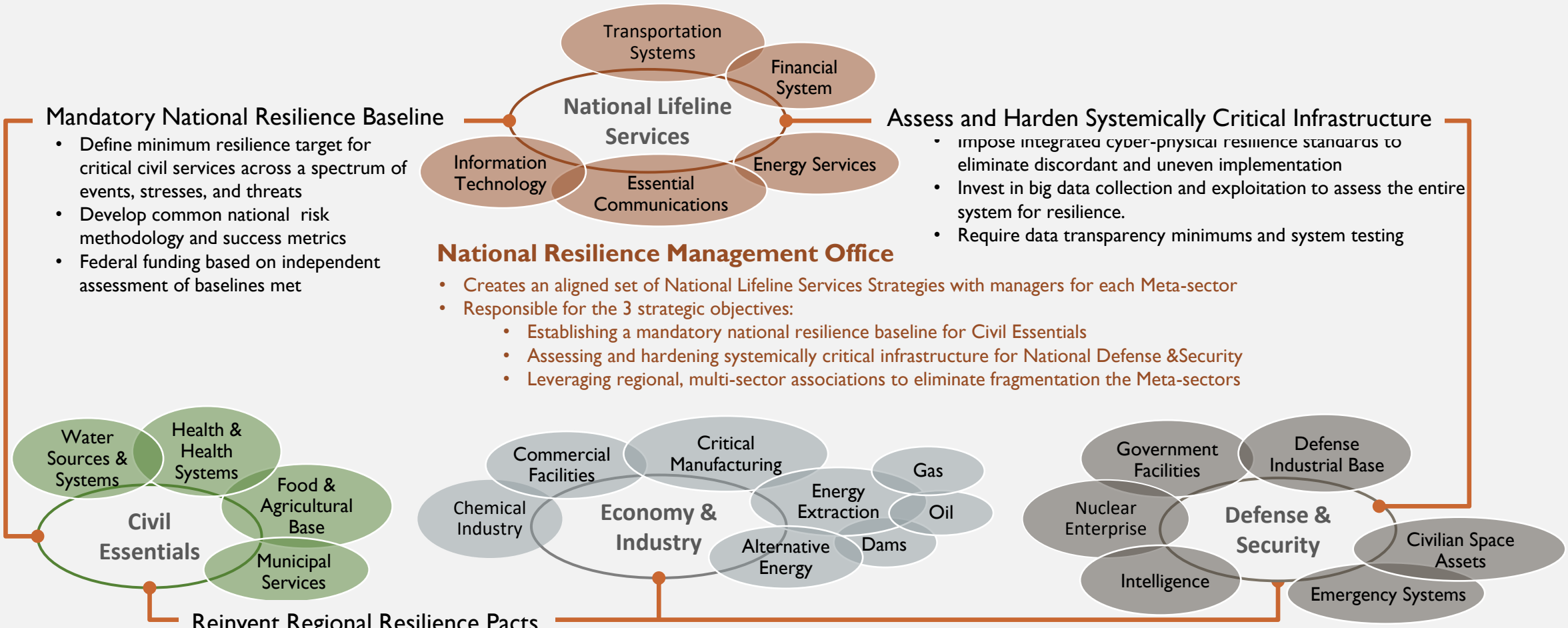
This Meta-sector is simultaneously the most diverse and specialized Meta-sector due to the variety of industries considered critical to manufacturing. Highly proprietary and competitive, there are trust issues to overcome in addition to USG understanding what the many components require for support.



The resilience of each sector and Meta-sector can be improved by mapping critical needs, dependencies, risks, and mitigation aspects for policy and strategy alignment to better manage resources and improve resilience.

The Role of a National Resilience Management Office

This graphic sets a strategic role for a separate federal office or agency that acts as a policy and program center for aligning the Meta-sectors.



Mandatory National Resilience Baseline

- Define minimum resilience target for critical civil services across a spectrum of events, stresses, and threats
- Develop common national risk methodology and success metrics
- Federal funding based on independent assessment of baselines met

Assess and Harden Systemically Critical Infrastructure

- Impose integrated cyber-physical resilience standards to eliminate discordant and uneven implementation
- Invest in big data collection and exploitation to assess the entire system for resilience.
- Require data transparency minimums and system testing

National Resilience Management Office

- Creates an aligned set of National Lifeline Services Strategies with managers for each Meta-sector
- Responsible for the 3 strategic objectives:
  - Establishing a mandatory national resilience baseline for Civil Essentials
  - Assessing and hardening systemically critical infrastructure for National Defense &Security
  - Leveraging regional, multi-sector associations to eliminate fragmentation the Meta-sectors

Reinvent Regional Resilience Pacts

- Reinvest in regional associations with shared modeling, exercises and risk assessments that develop systemic integration and regional resilience
- Increase funding for coordinated, regional resilience improvements with oversight by Critical Infrastructure Partnership Councils base on new sector structure.

Increased federal oversight, priority setting, funding, and planning are essential at the National Lifelines level to eliminate the disparate and uneven application of current and future sector guidance that improves infrastructure resilience.

John Rodman, Strategy Futures Reimagined, LLC

Reimagine the Federal Role in Critical Infrastructure Resilience

The bottom line is that decentralization of responsibilities for critical infrastructure at the U.S. scale is insufficient for resilience and requires governance, long-term funding, and designated authorities for:

- Aligning the uneven implementation of cyber and physical security across state, local, and private entities;
- Increasing expenditures in data collection, curation, management, and sharing that analyzed data through a common operational picture;
- Building and maintaining national risk, threat, and vulnerability baselines and remedies with penalties for noncompliance;
- Establishing protocols for international and national reconciliation of connected and integrated systemic risks due to inherent weaknesses in the critical infrastructure system or adversarial actions.

These functions require reimagining national management and strategy with increased funding and oversight, possibly independent of any current department or agency.

Infrastructure resilience in the U.S. must be continually funded, expertly managed, and methodologically-based to achieve measurable results for the future. A national effort with Federal governance and committed local partners.