Critical Infrastructure: No power

"Critical infrastructures are those infrastructure systems and assets that are so vital that their incapacitation or destruction would have a debilitating effect on security, the economy, public health, public safety, or any combination thereof."

- Why look at CI (PPD 21, EOs, SSA/SRMA, Cabinet Officials have SSA/SRMA authority)
- Almost Everything is CI
- Not CI: People, Fuel, Backup Generation, Military, Governance
- Individual vs CI
- Lifeline CI…

Why this paper: "There is a lack of understanding of the cascading, cross-sector interdependencies between infrastructure and what that means for prioritizing backup generation and other limited resources to maintain services and functions during a long-term, widespread outage."- The President's National Infrastructure Advisory Council

- Some CI focus on internal infrastructure

"Current planning frameworks focus on sector-by-sector preparedness and response, but in a catastrophic power outage, U.S. infrastructure and services will fail as a system. We need to take a systems approach—from the federal level down to the local level—to plan, design, and respond to these never-before-experienced events. This approach must move beyond existing planning and response frameworks and provide the guidance needed for an integrated cross-sector, cross-government strategy."- The President's National Infrastructure Advisory Council

- Horizontal vs vertical planning

Critical Infrastructure: No power

Paper: Focus on “time to failure” but need info and organization to arrive at time analysis

Supports CI and CI planners

Define the CI
- Sector Specific Plans (2010-2015)

What are the subsectors
- Subsector fail = sector failure
- Plan for subsectors

What are the Supporting Sectors
- Required for a given Sector to function

Subsector and Sector failure timelines (portrayed and discussed)

Impact/Recommendation

Grid Vulnerability Assessment

An assessment of the vulnerabilities of the grid shows that there are many sections/elements of the grid that can be attacked thereby creating a BSE. The table shows the grid entities that are vulnerable to the previously described threats. Several “threat types” overlap as the larger sections (e.g. Interconnects) are made up of smaller elements (e.g. transformers) and both are assessed. A more detailed analysis published by “Secure the Grid Coalition” is available at: https://securethegrid.com/wp-content/uploads/2024/05/Grid-Vulnerability-Assessment.pdf

Red means a high chance of creating a BSE, yellow means a potential chance of creating a BSE, green means little chance of creating a BSE (attacking multiple sections/elements simultaneously would increase threat impact).

Threat type	Physical	Cyber	HEMP	GMD
Threat ability to create a Black Sky Event by attacking Balance				
Threat ability to create a Black Sky Event by attacking Interconnects				
Threat ability to create a Black Sky Event by attacking Microgrids				
Threat ability to create a Black Sky Event by attacking Energy Economics/Markets				
Threat ability to create a Black Sky Event by attacking Generation				
Threat ability to create a Black Sky Event by attacking Transmission				
Threat ability to create a Black Sky Event by attacking Distribution				
Threat ability to create a Black Sky Event by attacking Control Centers/Balancing Authorities				
Threat ability to create a Black Sky Event by attacking Power Lines (conductors)				
Threat ability to create a Black Sky Event by attacking Towers				
Threat ability to create a Black Sky Event by attacking SCADA				
Threat ability to create a Black Sky Event by attacking Transformers				
Threat ability to create a Black Sky Event by attacking Transmission Breaker Stations				
Threat ability to create a Black Sky Event by attacking Grid Workers				
Threat ability to create a Black Sky Event by attacking Electricity Customers				

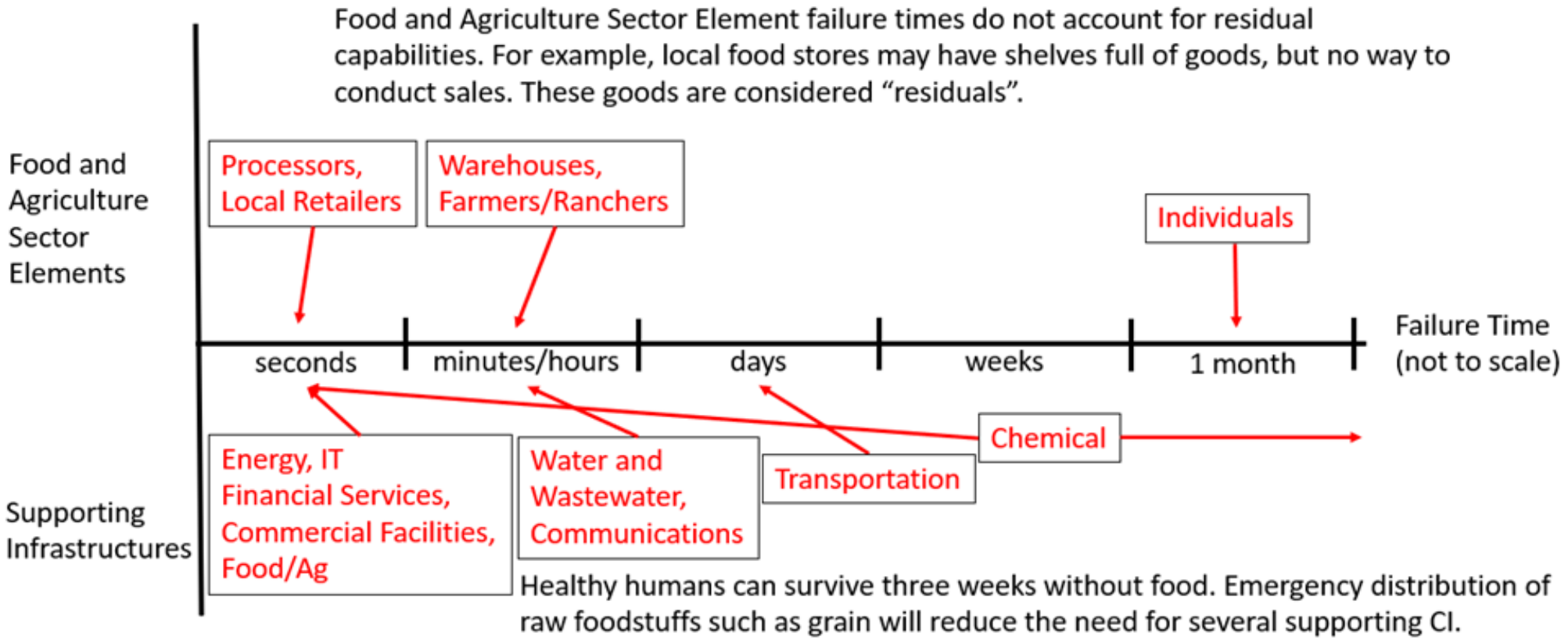
Assessment of Critical Infrastructure with No Grid Power

Every Critical Infrastructure (except perhaps Dams) fails without electricity. Many fail immediately while others take longer. Some can be classified as overwhelmingly failing while others have aspects that fail at different times. For example, “Financial Services” fails immediately and overwhelmingly without power while “Food” fails over a period of time as food stocks are depleted and starvation sets in.

The table depicts the general failure times for each CI without power. The United States Government published Sector Specific Plans (SSP) that included wording stating that each sector was reliant on electricity. While the reliance on electricity was clearly stated, the timeline to failure was not. These timeline estimates were derived from a study of each CI combined with subject matter expert review. A detailed analysis published by “Foundation for Infrastructure Resilience” is available at: https://img1.wsimg.com/blobby/go/0036af51-ee7e-4f71-a773-05dff2f7ed37/downloads/3fb43b54-1d82-4dcc-9e75-e3cc20e86007/Assessment%20of%20Critial%20Infrastructure%20With%20No%20G.pdf?ver=1742229490594

Critical Infrastructure (CI)	Failure Within Seconds	Failure Within Minutes/hours	Failure Within Days	Limited Failure
Chemical				
Commercial Facilities				
Communications				
Critical Manufacturing				
Dams				
Defense Industrial Base				
Emergency Services				
Energy				
Financial Services				
Food and Agriculture				
Government Facilities				
Healthcare				
Information Technology				
Nuclear				
Transportation				
Water and Wastewater				

Example: Food



What to do: Plan…then harden!

- Federal
- State
- Local