INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

RATIONALE AND PROCESS FOR

CONTINUITY OF THE ECONOMY

Institute for Homeland Security

Sam Houston State University

Benjamin L. Ruddell

Rationale and Process for Continuity of the Economy

Benjamin L. Ruddell, Ph.D., P.E.

July 20th, 2023

Table of Contents

Abstract

A regional economy is a vibrant ecosystem comprising critical infrastructures and economic agents like power and telecommunications, ports and logistics, networks of producers and suppliers, human capital, and government agencies. In the increasingly connected and chaotic global economy, resilient regional economies must implement economic development and regulatory policies that ensure "Continuity of the Economy" (COTE) during major social, economic, or environmental shocks. COTE requires that all providers and operators of critical infrastructures and critical functions establish adequate capacity to self-recover after a major disruption and prepare adequate input supply chain buffers so that supplier disruptions do not take down critical services before the economic network can recover itself. Non-critical suppliers support interdependent critical infrastructures, blurring the artificial lines between critical and non-critical sectors and highlighting the need for a cross-cutting whole-of-economy approach instead of a sectoral approach to preparedness. This whole-of-economy planning and preparation is made possible by implementing a recurring community-based participatory process that maps supply chains, measures buffers and recovery requirements, and connects critical infrastructure service providers and recovery responders directly with suppliers to share recovery priorities and plans. This participatory process also screens out non-critical suppliers that are not necessary in the short term to recover or sustain critical infrastructures and critical functions during a major disruption, enabling recovery operations to focus on critical infrastructures and critical suppliers and speed recovery. Establishing adequate supply chain buffer time and inside-out recovery capacity are identified as the key foci for COTE preparedness. COTE is an all-hazard approach to resilience and preparedness that complements existing economic development, five-year emergency planning, cyber preparedness, and emergency management processes.

Keywords

Continuity of the Economy, COTE, Emergency Management, Defense, Planning, Process, Supply Chain, Critical Infrastructure, National Critical Functions, Whole of Economy, Regulation, Communication, Resilience, Response, Recovery, Buffer, Inventory.

Rationale and Process for Continuity of the Economy

Benjamin L. Ruddell, Ph.D., P.E.

July 20th, 2023

Executive Summary

Since September 11th, 2001, a great deal of energy has been directed by the U.S. Federal Government to enhance homeland security and resilience. Numerous executive directives and agency policy documents have been issued, including for example the USA Patriot Act (2003), PPD-21 (2013), Executive Order 13806 (2017), Goal 3 of the National Strategy for Advanced Manufacturing (2022), the Supply Chain Resilience Guide (2019), the Executive Order on America's Supply Chains (2021), and the creation of the Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA). These federal actions emphasize that resilient critical infrastructure and resilient supply chains are prerequisite for a secure population and economy that is prepared to quickly respond to and recover from all kinds of catastrophes.

The concept of the Continuity of the Economy (or COTE) recognizes that the operators of critical infrastructures and their supporting supply chains are on the front lines of planning, response, and recovery from a major catastrophe that is large enough to damage or exhaust the recovery capacity of governmental emergency management or its supporting private sector supply chain. In such an eventuality rapid and effective government coordination with the private sector is required to avert systemic collapse. A well-exercised COTE plan integrates the objectives of emergency management, business continuity, supply chain resilience, and critical infrastructure security into a complete public-private strategy for resilience to catastrophes. In recognition of the fundamentally unpredictable nature of major catastrophes, the foundation of COTE is the maintenance and sharing of adequate information about the structure of and recovery plans for supply chains and critical infrastructures in the community along with the maintenance of relationships between the operators of the various systems.

Every 21st century U.S. community needs a Continuity of the Economy plan to satisfy the federal guidelines and rules mentioned above, and to develop a resilient economy that can weather the disruptions of this unpredictable 21st century. Economic continuity is a key to population protection and security, but it is also a major competitive advantage and deterrent against attack in a chaotic global environment. This paper explains why COTE is required and then introduces a formal process available today that implements current federal guidelines.

Key points argued in this paper include:

1. Continuity of the Economy (COTE) establishes the capacity of the whole economic network to self-recover from the inside out after a major disruption.
2. The sixteen U.S Critical Infrastructure sectors depend on supply chains outside those sectors;
3. Critical infrastructures exist to support critical supply chains, so supply chain concepts elegantly complement critical infrastructure and critical function resilience planning, unifying the concepts;
4. Supply chains are not critical if a critical infrastructure can be operated and recovered without them;
5. The criticality of a supply chain can be measured as "Buffer Time" before its disruption is felt, and especially before disruption to a critical function or infrastructure is felt;

6. The purpose of a COTE plan is to reduce supply chain criticality by (a) reducing recovery time through preparation, (b) adding buffer time for critical infrastructures to recover their supply chains, (c) deprioritizing non-critical supply chains from the recovery process so resources can focus on recovering the most critical supply chains, and (d) overcoming the limitations of the sectoral "critical infrastructure" and "critical functions" paradigm that limits coordination and creates supply chain blind spots;
7. A COTE planning process should implement and support DHS processes for emergency management, critical infrastructure, critical functions, community disaster resilience zones, the five-year planning process, and supply chain resilience, along with other applicable processes;
8. Government emergency response and recovery organizations should focus first on ensuring that the whole of the economy is prepared to support COTE during a major disruption, because during a major disruption the government's assets will be vanishingly inadequate… COTE provides a large force multiplier to the government's recovery capacity;
9. Participatory planning processes such as the FEWSION for Community Resilience process (F4R) support COTE planning and exercises using tools and data available today, making COTE planning accessible to small, medium-size, rural, tribal, and territorial communities without the specialized resources that the largest cities and corporations dedicate to resilience planning; and
10. Anyone operating or regulating a critical infrastructure, or a supply chain supporting a critical function, should regularly complete a COTE planning and investment process so they are prepared with the information, inside-out self-recovery capacity, and supply chain buffers necessary to recover the critical functions of the economy during a widespread disruption.

Rationale and Process for Continuity of the Economy

Benjamin L. Ruddell, Ph.D., P.E.

July 20th, 2023

1. Supply Chains and Critical Infrastructures in the Economy

How does the economy function? The economy is structured into a "hierarchy of needs" where value-added economic activities, including services and manufacturing, are supported by natural resource exploitation. The four major sectors are outlined in Table 1. The Primary sector extracts and exploits natural material resources; the Secondary sector adds value including via manufacturing to convert those natural resources into useful finished goods; the Tertiary sector provides services that directly add value or effectiveness to those finished goods; and the Quaternary sector provides services that govern or improve the other three levels. Figure 1 presents the relative size of the various sectors, emphasizing that (1) value-added sectors are much larger than primary sectors, and (2) the government including its recovery and emergency management functions has a tiny fraction of the capacity of the private sector(s).

Table 1: The four major sectors of the economy, with examples given for each sector.

- Primary (extraction of natural resources)
  - Farming and Forestry
  - Fishing
  - Mining
  - Energy Production, e.g. Oil, Natural Gas, Solar, Wind, Uranium
  - Raw water; Dams, canals, and wells
- Secondary (production of finished goods and value-added materials)
  - Manufacturing
  - Energy and Water Utilities, e.g. potable water, electricity, and natural gas
  - Construction
- Tertiary (delivery of services)
  - Trade of finished goods, wholesale and retail
  - Finance and Banking
  - Cyber, Communications, and Information Technology
  - Sports, Recreation, and Tourism
  - Transportation and Distribution of finished goods
  - Healthcare
  - Security
  - Waste & Wastewater Management
  - Emergency Management
- Quaternary (services that improve or govern the other three sectors)
  - Education (scientific, professional, religious, humanities)
  - Research and Development
  - Government

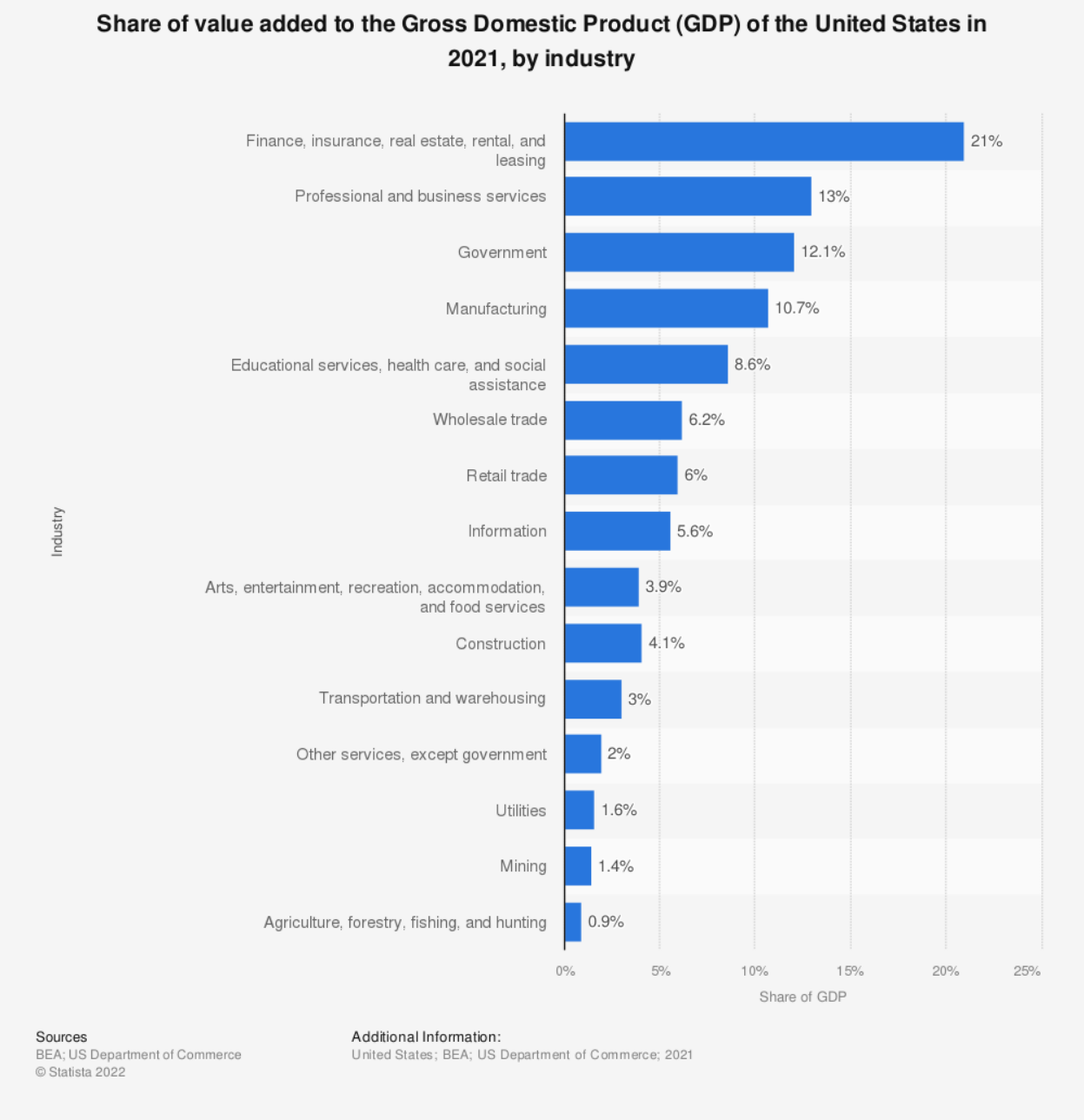

Figure 1: The relative size of various sectors of the U.S. economy in 2021, as a share of GDP (percentage)[1]. Observe that value-added sectors are much larger than primary sectors, and that the government has far less size and capacity than the private sector(s).

A supply "chain" is more correctly understood not as a linear chain but as a circular web of flows of goods and services divided into roughly seven major stages and linking all entities in the economy, including the operators of critical infrastructures. Figure 2 presents the FEWSION project's generalized supply chain model. Constitutive goods and services are extracted (E) from raw materials, transformed through a production step (P), moved through Storage (S) and Distribution (D), brought to market in

[1] BEA, US Department of Commerce, 2021, ©Statista 2022.

finished form (R), consumed (C), and discarded and/or recycled (W). Emergency management operations and critical functions tend to occupy stages three through six but are especially concentrated in stages four and five (distribution and retail). The supply chains supporting emergency management operations and critical functions tend to comprise stage two three and four services (production, storage, and distribution).

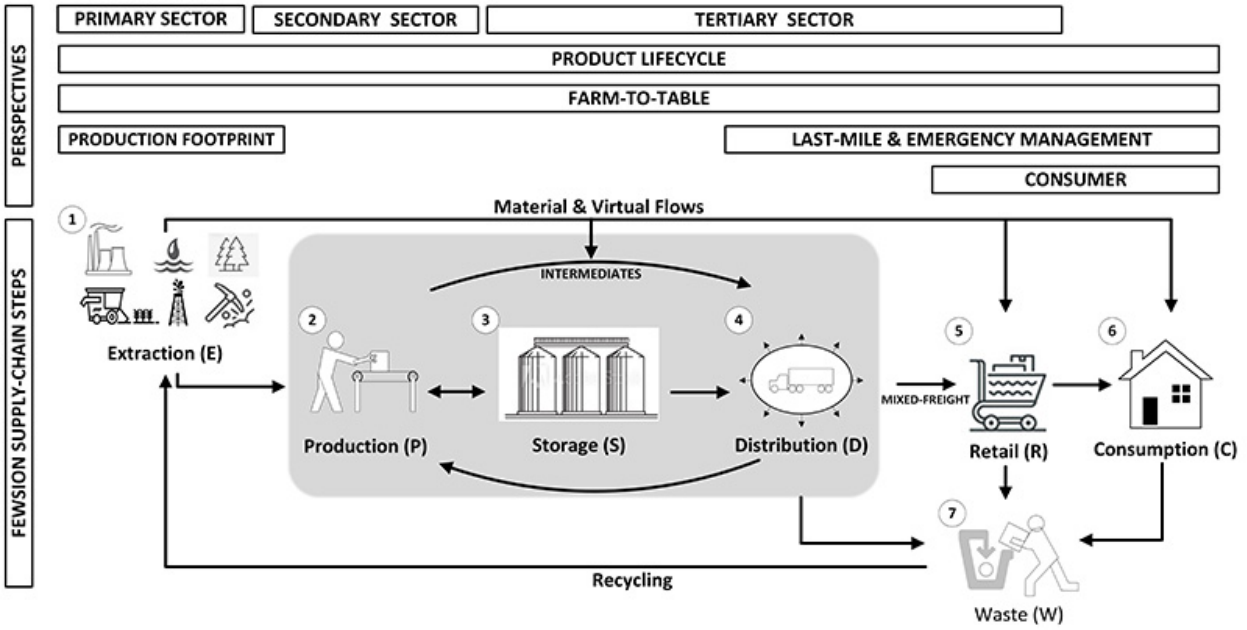

Figure 2: The FEWSION general supply chain model[2] follows common practice by defining seven major stages of a supply chain. Reproduced with permission of the authors. Sector-specific supply chain diagrams are available from FEWSION via the website https://fewsion.us.

The term "critical infrastructure" is defined in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), as:

> *"... systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."*

All four economic sectors support supply chains that sustain critical infrastructures. Critical infrastructures and their operators tend to occupy the secondary and tertiary levels, and mostly provide critical tertiary services like transportation, healthcare, security, water, power, communications, or payments. The suppliers and supply chains of critical infrastructures are concentrated in the secondary economic sector. Critical infrastructures can operate for a limited amount of "Buffer" time without their supporting supply chains; days without food; milliseconds without power. When critical infrastructures have more "time on hand" (ToH) of supply chain inputs from other layers and sectors of the economy, they can sustain operations for a longer buffer time. But, eventually, most goods and services in the economy are needed in order to sustain critical infrastructure operations; even the quaternary sector services of the U.S. Congress will eventually be needed to govern critical infrastructures. The shorter the

[2] Ruddell, B.L., H. Gao, O. Pala, R. Rushforth, and J. Sabo, Figure 10.1 (general supply chain) from Chapter 10; Infrastructure, in P. Saundry and B.L. Ruddell (eds.), The Food Energy Water Nexus, Springer, 2019 (in press).

buffer time before disruption of critical functions and/or life-or-death consequences ensue, the more "critical" the service or its supply chain becomes. Some sectors, like power and communications, cannot be interrupted at all without major consequences and critical function failures.

Executive Order 14017 defines "… critical goods, products, and services." using similar language that earlier federal actions have used to define critical functions and critical infrastructures. Critical infrastructures are themselves part of the supply chain, and in turn require resilient supply chains in order to function during emergencies. The critical infrastructure sectors for which the Cybersecurity and Infrastructure Security Agency (CISA) is concerned are listed in Table 2 below, along with the "Sector-Specific Agencies" (SSAs) responsible for government oversight of each category of critical infrastructure. Note in Table 2 that the Department of Homeland Security, and by extension the Federal Emergency Management Agency (FEMA) and CISA, are the SSA for most critical infrastructure sectors, so FEMA and CISA are key agencies responsible for emergency management of critical infrastructure and its operators.

Table 2: CISA Critical Functions and/or Critical Infrastructures, and their sector-specific U.S. Federal Agencies, reproduced from PPD-21[3]; note that cyber-functions are being added to a forthcoming update of PPD-21 as of 2023, along with other changes.

Chemical: Department of Homeland Security
Commercial Facilities: Department of Homeland Security
Communications: Department of Homeland Security
Critical Manufacturing: Department of Homeland Security
Dams: Department of Homeland Security
Defense Industrial Base: Department of Defense
Emergency Services: Department of Homeland Security
Energy: Department of Energy
Financial Services: Department of the Treasury
Food and Agriculture: U.S. Department of Agriculture and Department of Health and Human Services
Government Facilities: Department of Homeland Security and General Services Administration
Healthcare and Public Health: Department of Health and Human Services
Information Technology: Department of Homeland Security
Nuclear Reactors, Materials, and Waste: Department of Homeland Security
Transportation Systems: Department of Homeland Security and Department of Transportation
Water and Wastewater Systems: Environmental Protection Agency

The relationship of supply chains with critical infrastructures, national security, and emergency management is addressed by Executive Order 14017[4] on America's Supply Chains:

> *"The United States needs resilient, diverse, and secure supply chains to ensure our economic prosperity and national security. Pandemics and other biological threats, cyber-attacks, climate shocks and extreme weather events, terrorist attacks, geopolitical and economic competition, and other conditions can reduce critical manufacturing capacity and the availability and integrity of critical goods, products, and services."*

[3] PPD-21, Presidential Policy Directive – Critical Infrastructure Security and Resilience, February 12th 2013, Accessed May 2nd 2023 at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[4] Executive Order 14017, America's Supply Chains, February 24th 2021. Accessed May 2nd 2023 at: https://www.federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chains

Critical infrastructures and their operators are properly understood as components of the economic network, and as both "upstream" and "downstream" participants in the supply chain that operates the critical functions for the economy. Therefore, to recover and sustain disrupted critical infrastructures and critical functions, we must also recover and sustain the supply chains that lie upstream of the critical functions. The fifty-four National Critical Functions (NCF)[5] are the outcomes supported by Critical Infrastructures:

> *"National Critical Functions (NCFs) are functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."*

The NCF concept shifts the emphasis away from the "structure-focused" or "entity-focused" U.S. National Critical Infrastructure framing and instead places the emphasis on the outcomes delivered and functions carried out by the U.S. National Critical Infrastructures. There are four categories of NCFs: connect, distribute, supply, and manage; the first three categories are explicitly supply chain functions. It is clear that NCFs, supply chains, and critical infrastructures are closely aligned concepts requiring deliberate integration.

In summary, the shift to the NCF framing emphasizes that we need planning and management processes that view the system as an interdependent network and that breaks down bureaucratic distinctions between the sectors. The "criticality" of a critical function or supply chain is better understood as an amount of time before severe consequences ensue dur to disruption of critical functions, rather than as a sectoral label. Some "non-critical sector" supply chains are more critical than "critical infrastructures" because a critical function will rapidly fail without that supply. It is more important and also arguably simpler that an operator manages and communicates its buffer times and recovery priorities with its own suppliers and customers than that the operator knows whether those connections are officially labeled as "critical".

2. Resilience of an Economy to Shocks

The purpose of the national conversation about Critical Infrastructures and National Critical Functions is to create resilience to shocks and disruptions in the economy. What, then, is resilience? Resilience is an intuitive concept but also one that has many different academic definitions[6], such as resistance to change, robustness to a wide variety of threats, and recovery from damage. At the root of the concept of resilience lies the adaptive learning cycle. Natural ecosystems achieve "learning" through unplanned evolutionary trial and error, so more diverse[7] ecosystems are more resilient[8] and stable through shocks and stresses because they have more opportunities to adapt to the circumstances. The economy is a type of ecosystem-that is, the economy is a Socio-Ecological-Technical System (SETS[9] [10] [11]) or Coupled Natural Human

[5] CISA (2019), National Critical Functions Overview, April 30 2019, https://www.cisa.gov/national-critical-functions

[6] Lewis, "The Many Faces of Resilience", 2022.

[7] Holling, C. S. 1973. Resilience and stability of ecological systems. Annu Rev Ecol Syst 4:1-23.

[8] Isbell, F. et al. Biodiversity increases the resistance of ecosystem productivity to climate extremes. Nature 526, 574–577 (2015).

[9] Chester, M., Underwood, B.S., Allenby, B., Garcia, M., Samaras, C., Markolf, S., Sanders, K., Preston, B. and Miller, T.R., 2021. Infrastructure resilience to navigate increasingly uncertain and complex conditions in the Anthropocene. Npj Urban Sustainability, 1(1), pp.1-6.

[10] Kim, Y., Carvalhaes, T., Helmrich, A., Markolf, S., Hoff, R., Chester, M., Li, R. and Ahmad, N., 2022. Leveraging SETS resilience capabilities for safe-to-fail infrastructure under climate change. Current Opinion in Environmental Sustainability, 54, p.101153.

System (CNHS[12]). The ecological principles governing resilience to shocks[13] fully apply[14] to the operations[15] of the economic ecosystem[16].

However, people and their organizations can be more resilient than natural ecosystems, at least in principle, by forecasting shocks and stresses and learning to adapt their behavior before those events occur. Scientific advances, when translated into monitoring systems and predictive models, are key tools for anticipatory adaptation in the modern world. Traditional social values and cultural structures likewise have significant merit for anticipatory resilience to the extent that they embody the empirical experiences and expectations learned "the hard way" during thousands of years of human civilization. Modern management processes are also (among other things) attempts to achieve resilience and balance it against other objectives. As an early formal example, Drucker's management principles embrace the practice of observation and measurement as a basis of sound decision making[17]. Boyd's OODA loop[18] (Observe Orient Decide Act) was born of the need to quickly adapt in order to survive the competition of aerial combat in Vietnam. Hollnagel's Resilience Analysis Grid[19] (RAG) formally linked the learning cycle with organizational resilience by defining an organization's resilience in terms of a cycle including the capacity to monitor, anticipate, respond, and learn in a changing environment. The foundation of resilient critical functions is the ability of the collective organizations operating critical infrastructures and supply chains to effectively learn and adapt[20].

The U.S. Government has been adapting and learning from decades of military, political, and economy shocks. The federal agency missions and regulations now emerging are part of a learning cycle that arguably started with September 11th, 2001, and with the USA Patriot Act of that year. For example, the 2013-year PPD-21 defines resilience as, "… the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.". Current and forthcoming federal reforms are an attempt to put this learning into practice, with an emphasis on building resilience against the most common and consequential hazards. Examples include defining and measuring risk from the eighteen natural hazards considered in the National Risk Index[21], or the establishment of FEMA Community Disaster Resilience Zones, the administration of the FEMA Five

---

[11] Markolf, S.A., Chester, M.V., Eisenberg, D.A., Iwaniec, D.M., Davidson, C.I., Zimmerman, R., Miller, T.R., Ruddell, B.L. and Chang, H., 2018. Interdependent infrastructure as linked social, ecological, and technological systems (SETSs) to address lock-in and enhance resilience. Earth's Future, 6(12), pp.1638-1659.

[12] Turner BL, Kasperson RE, Matson PA, McCarthy JJ, Corell RW, Christensen L, Eckley N, Kasperson JX, Luers A, Martello ML, Polsky C, Pulsipher A, Schiller A (2003) Science and technology for sustainable development special feature: a framework for vulnerability analysis in sustainability science. Proc Natl Acad Sci 100:8074–8079.

[13] Gomez, M., Mejia, A., Ruddell, B.L. and Rushforth, R.R., 2021. Supply chain diversity buffers cities against food shocks. Nature, 595(7866), pp.250-254.

[14] Walker, B., C. S. Holling, S. R. Carpenter, and A. Kinzig. 2004. Adaptability and Transformability in Social-Ecological Systems. Ecology and Society 9:5.

[15] Helfgott, A. Operationalising systemic resilience. Eur. J. Oper. Res. 268, 852–864 (2018).

[16] Nyström, M. et al. Anatomy and resilience of the global production ecosystem. Nature 575, 98–108 (2019).

[17] Drucker, P.F., 1971. What we can learn from Japanese management.

[18] Boyd, John R. (3 September 1976). Destruction and Creation (PDF). U.S. Army Command and General Staff College.

[19] Hollnagel, E., 2010, May. How resilient is your organisation? An introduction to the resilience analysis grid (RAG). In *Sustainable transformation: Building a resilient organization*.

[20] Seager, T.P., Clark, S.S., Eisenberg, D.A., Thomas, J.E., Hinrichs, M.M., Kofron, R., Jensen, C.N., McBurnett, L.R., Snell, M. and Alderson, D.L., 2017. Redesigning resilient infrastructure research. In Resilience and risk (pp. 81-119). Springer, Dordrecht.

[21] FEMA (2023), National Risk Index, March 2023.

Year Planning Process, the creation of CISA, Executive Order 13806[22] on manufacturing supply chain resiliency, the National Strategy for Advanced Manufacturing[23], or the enhancement of regulations focused on resisting the natural hazards considered by engineers in the design of robust civil infrastructures.

Three common dimensions of resilience are the "Three R's"[24]: Resistance to disruption, capacity to execute Recovery after a disruption, and Robustness of our strategies to handle a wide variety of hazards. By improving each of the Three R's, we reduce our risk. Recovery capacity is arguably a more robust approach than resistance because it is difficult and expensive to implement resistance strategies that are robust against a wide range of threats, whereas recovery capacity tends to be more robust regardless of the nature of the threat. But, threat-specific resistance is usually the most cost-effective strategy where threats are known in advance. Therefore, in the past we have emphasized threat prevention and vulnerability reduction to resist historically frequent hazards and reduce risk posed by those hazards, where risk is measured using the RAMCAP[25] approach as Risk = Vulnerability x Threat x Consequence. It is cost-effective to build resistance to well-understood threats by buying down our vulnerability to threats (reducing Vulnerability) and by predicting and avoiding threats (reducing Threat probability), as well as by reducing the extent of our exposure to these threats (reducing Consequence). Unfortunately, many critical infrastructure failures involve "Black Swan"[26] events that were not anticipated, could not be anticipated, were designed to exploit asymmetric vulnerabilities, or will never occur again in the same way. The RAMCAP approach to building resilience by building resistance to historically frequent threats is not very effective for Black Swans.

Large, rare hazards tend to be poorly understood, or merely forgotten, so the human tendency toward "recency bias" and misuse of statistics set us up for failure when it matters the most- in major disasters or attacks[27]. Matters are worse for "nonstationary" hazards for which even the best historical data is irrelevant because the facts have shifted since the data was collected[28]. Matters are nearly impossible for adversarial threats in a COTE context, because the whole of the economy is an impossibly soft target with a huge threat perimeter[29] against which an intelligent adversary can easily apply asymmetric force and can easily switch tactics to circumvent hardening countermeasures. We now appreciate asymmetric threats following the events of September 11th, 2001, and the massive wave of cyberthreats unfolding at present. Additionally, failures can and do occur when protection strategies fail to address fully anticipated threats such as Hurricane Katrina, Winter Storm Uri, and the 2023 earthquake in Southeast Turkey. There will always be failures that we did not anticipate and could not harden ourselves against. Unfortunately, we have learned that Black Swans tend to be the same severe shocks that create high-consequence cascading failures throughout the economy, so Black Swans cannot be neglected in our resilience processes.

---

[22] Trump (2017), Executive Order 13806—Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States, July 21st 2017.

[23] NSTC (2022), National Strategy for Advanced Manufacturing, National Science and Technology Council, October 2022.

[24] Allen, C. R., Angeler, D. G., Chaffin, B. C., Twidwell, D. & Garmestani, A. Resilience reconciled. Nat. Sustainability 2, 898–900 (2019).

[25] Brashear, J.P. and Jones, J.W., 2010. Risk analysis and management for critical asset protection (RAMCAP plus). Wiley handbook of science and technology for homeland security, 2, pp.1-15.

[26] Taleb, N.N., 2007. The black swan: The impact of the highly improbable (Vol. 2). Random house.

[27] Bilginsoy, Z. and S. Fraser (2023), Turkey's lax policing of building codes known before quake, Associated Press, February 10th 2023. Accessed May 10th 2023 at: https://apnews.com/article/politics-2023-turkey-syria-earthquake-government-istanbul-fbd6af578a6056569879b5ef6c55d322

[28] Milly, P.C., Betancourt, J., Falkenmark, M., Hirsch, R.M., Kundzewicz, Z.W., Lettenmaier, D.P. and Stouffer, R.J., 2008. Stationarity is dead: Whither water management?. Science, 319(5863), pp.573-574.

[29] Bennett, B.W., Twomey, C.P. and Treverton, G.F., 1999. What Are Asymmetric Strategies. RAND NATIONAL DEFENSE RESEARCH INST SANTA MONICA CA.

As a result, a comprehensive resilience strategy must cost-effectively combine threat-specific Resistance strategies with more robust "all-hazards" resilience strategies that do not require accurate anticipation of a threat or mitigation of vulnerability to that threat. All-hazards resilience strategies do not replace threat-specific hardening and "primary" failure prevention strategies (Table 3), if only because threat-specific hardening tends to be very cost effective. Instead, all-hazards resilience strategies emphasize containment of and recovery from primary failures and emphasize the prevention of "secondary" cascading failures that geometrically expand risk via network dependencies[30], regardless of the cause of the primary failure (note: do not confuse secondary failure with the secondary sector of the economy). In other words, secondary resilience strategies focus on resisting the cascade of failures through the network and on recovering that cascade, rather than focusing on resisting the primary failure. Keeping failures small and localized and recovering them quickly is a strategy that works for a wide range of threats and hazards and tends to be cost-effective. The network resilience methods developed by Ted Lewis are a good example of all-hazard network resilience thinking implemented in practice (e.g. Lewis 2022).

It is also important to understand the role of the supply chain and critical infrastructure network topology in the creation of all-hazards resilience. Since Baran's pioneering studies on communication networks in 1962[31], it has been understood that centralized networks are highly vulnerable to targeted attacks at their hubs, whereas distributed networks are much more resistant disconnection due to both targeted and random threats (Figure 3). The ideal network for resilient supplier connectivity is a distributed "small world"[32] network where your organization has a variety of suppliers both near and far and both large and small. This sort of network has the ability to move supplies across distances efficiently, but also creates a diversity of options for supply and for recovery of the network regardless of whether the hazard is localized or widespread. The more centralized your supply chain becomes, the less resilient it becomes[33]. In the extreme instance where every organization depends on a single supplier, the whole system can be taken down by the failure of that one supplier; this is a very fragile system. Single-supplier supply chains, monopolistic suppliers, and geographically concentrated supply chains are inherently fragile in the face of all kinds of hazards both random and targeted.

[30] Lewis, T.G., 2019. Critical infrastructure protection in homeland security: defending a networked nation. John Wiley & Sons.

[31] Baran, P., 1962. On Distributed Communications Networks, First Congress of the Institute for Information System Sciences.

[32] Watts, D.J. and Strogatz, S.H., 1998. Collective dynamics of 'small-world'networks. nature, 393(6684), pp.440-442.

[33] Albert, R., Jeong, H. and Barabási, A.L., 2000. Error and attack tolerance of complex networks. nature, 406(6794), pp.378-382.

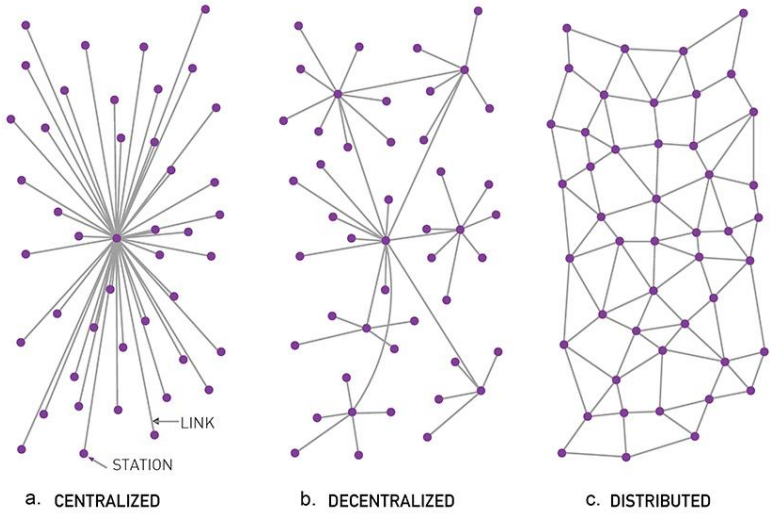

Figure 3: Baran's 1962 study of network topology. Distributed networks are the most resilient to both random and (especially) targeted disruptions, especially if they combine a diversity of localized connections with cross-network "small world" connections.

It should now be clear why all-hazards resilience strategies are so important for COTE, and why the keys to that all-hazards resilience are a distributed supply chain network topology, recovery capacity, and resistance to secondary cascading failures that take down networked critical infrastructures and supply chains, regardless of whether these networks are officially labeled "critical".

Table 3: Examples of threat-specific and all-hazard strategies for resilience.

Threat-Specific Resilience Strategies include,

- Defeating a threat before it becomes large,
- Anticipating and cost-effectively hardening against known threats to reduce vulnerability, and
- Favoring hardening strategies that are robust against multiple known threats.

All-Hazard Resilience Strategies include,

- Making systems "safe to fail"[34] where downstream dependencies are not very consequential,
- Increasing the "buffer time" using warning systems, backup options, and stockpiles to create enough time to recover supply chains and dependencies before failures cascade,
- Improving recovery speed with more recovery assets, better information on plans and priorities, and better bilaterial communications between suppliers and their dependents,
- Diversification of the supply chain so an unforeseen threat is less likely to affect all connections at once (e.g. Gomez et al. 2021),
- Increasing the "ramp rate" of adaptation so the network can outpace failures[35] by switching supply chain sources and restructuring the network,

[34] Ahern, J., 2011. From fail-safe to safe-to-fail: Sustainability and resilience in the new urban world. Landscape and urban Planning, 100(4), pp.341-343.

[35] Rushforth, R.R., Messerschmidt, M. and Ruddell, B.L., 2020. A Systems Approach to Municipal Water Portfolio Security: A Case Study of the Phoenix Metropolitan Area. Water, 12(6), p.1663.

- Restructuring the network to contain cascading failure by compartmentalizing, islanding, adding redundancy, and reducing highly connected hubs, and
- Keeping capital in reserve to pursue alternative strategies after the primary strategy fails, avoiding "sunk capital".

3. A Practical Approach to Achieve Continuity of the Economy

"Continuity of the Economy" (COTE) is an intuitive concept that solves the interdependency problem created by severe Black Swan shocks that create severe and widespread disruptions to critical functions via disruption of critical infrastructure and supply chain networks. How can the emergency management (EM), Department of Homeland Security (DHS), and Department of Defense (DoD) communities recover the nation's critical infrastructures after a major shock when these infrastructures depend on a wide variety of cross-sectoral private sector supply chains and functions that are outside the influence, scope, competence, and visibility of the responsible government agencies and the critical infrastructure operators? For example, how can we recover a damaged power grid if adequate transformer supply chains are unavailable, e.g. for oil or stamped casings used to build transformers? How are we to ensure that the economy's critical supply chains provide the goods and services needed to sustain and restore critical infrastructure, especially during a severe shock that causes damage across many sectors and regions?

The term "Continuity of the Economy" was coined by the Cyberspace Solarium Commission report[36] in 2020. The recommendations of that report were introduced as the Continuity of the Economy Act[37]. This Act or a future permutation thereof requires the Executive Branch to make provision for the continuity and recovery of the private sector systems that support homeland security and defense in the wake of a cascading failure in the US economy. Key language from this proposed legislation is provided below:

> *"[The Continuity of the Economy Act of 2020] requires the President to develop a plan to maintain and restore the U.S. economy in response to a cyberattack or other significant event that is natural or human-caused that results in severe degradation to economic activity. Among other requirements, this plan shall (1) examine the distribution of goods and services across the United States necessary for the reliable functioning of the country during such an event; (2) identify the economic functions of relevant actors whose disruption, corruption, or dysfunction would have a debilitating effect on security, defense readiness, or public health or safety; and (3) identify the critical distribution mechanisms for each economic sector that should be prioritized for operation during such an event."*

Who is responsible for ensuring the Continuity of the Economy during major disruptions? National-level resilience to catastrophes is the regulatory goal of CISA, FEMA, and related sectoral agencies. The Department of Defense does not have responsibility for the domestic resilience mission, but it has significant capacity to support domestic recovery operations when needed, and it has a significant interest in ensuring that domestic US supply chains are resilient enough to supply its operations during a crisis. Large businesses support business continuity and risk management functions that are essential for COTE, and the private sector hosts roughly 98% of the capacity to provide critical goods and services. State, Tribal, and Local government organizations take the lead on resilience and emergency response within their jurisdictions. In summary, every kind of organization that provides critical functions, or that supports the supply chains of critical functions, has some role in COTE. Most of the people and

[36] Cyberspace Solarium Commission (CSC) report, https://www.fdd.org/wp-content/uploads/2020/03/CSC-Final-Report.pdf

[37] Continuity of the Economy Act of 2020, 116th Congress, S.3928. Accessed May 2nd 2023 at: https://www.congress.gov/bill/116th-congress/senate-bill/3928/text

organizations in a nation are part of a web that supports critical functions via supply chains. Therefore, the "stovepiped" approach of assigning responsibility for COTE to one party and relieving another is unworkable for this problem. This huge, complicated, and interdependent system respects no clear boundaries, so every supplier and dependent in the system must take responsibility for their own COTE preparations and operations.

Adopting a network perspective based on supply chain thinking is a good start for an organization to address its COTE concerns, especially if data is readily available to map those networks for your community. However, focus is required. If everything in the economy is critical, nothing is critical. CISA's sixteen critical infrastructure sectors already encompass a large fraction of the economy. If we additionally consider the economy's critical supply chains necessary to sustain and recover those critical infrastructures, the result could be unmanageable. That is most of the economy. Complicating matters further, COTE must concern itself primarily with unpredictable Black Swan events, so it is not possible to predict or prevent the disruptions that will occur. How, then, are we to practically address the COTE problem in a complicated system without clear boundaries? Suggestions for the practical focus of the COTE exercise follow.

First, focus on proactively mapping and connecting the network of your own organization. The first step in learning to prevent cascading failures in the economic network is also the first step in the response and recovery process: each organization needs to understand its own dependencies and dependents, both those upstream supply chains it depends upon, and also the downstream supply chains it supports, along with the key people who are responsible for those connections. By mapping out the physical and social network connections in advance of a shock and communicating with the people responsible for those connections, an organization knows where to begin the planning and recovery processes and who to include in those processes.

Second, focus on inside-out recovery capacity, which is more robust than hardening. In a changing world of Black Swans and asymmetric threats, prevention and hardening against shocks is not always possible- especially not for the most severe and unprecedented shocks. Instead, ensure that recovery capacity is a focus in your organization and also in your suppliers' organizations. Form and communicate recovery plans to your upstream and downstream networks on a regular basis to accelerate response and to empower your suppliers to independently take the initiative on recovery without needing your direction or support from a government emergency manager. Recovery operations require equipment, personnel, and supplies; do not assume you will have access to any recovery assets during an emergency unless you already have them on hand. Prepare to recover "inside-out", starting with your resources on hand, and do not assume outside help will be quickly forthcoming. As an added benefit, you may find yourself with extra recovery assets on hand if you are not affected by the shock, and these will be helpful and profitable for mutual aid operations to your neighbors.

Third, focus on building appropriate buffers. Buffer time, or "time on hand" of needed equipment and supply inventory, is the single most important measurement for resilience and recovery in the context of cascading shocks on a supply chain network. Organizations with more supplies kept in the inventory, more backup supply options, and better have more time and choices available for recovery during a severe emergency. A supply chain or infrastructure is only critical if its disruption quickly results in severe consequences to your organization or community. The best way to address critical supply chain and critical infrastructure resilience problems is to make sure your organization has enough time available for response and recovery before anything becomes critical. Measure the number of hours that your organization can continue to provide its critical services, and/or can carry out response and recovery operations without access to each of your supply chains; this is each supply chain's buffer time. Estimate the recovery time it will take for your organization and other critical infrastructure operators in the area to accomplish recovery operations and restore minimal emergency services for each of your supply chains during a Black Swan event (this is impossible to do accurately, so be conservative). If a supply chain has

less buffer time than the associated recovery time for that supply chain, add buffer and/or add recovery assets to bring the recovery time down below the buffer time. If your organization's primary purpose is emergency management or recovery, build in a lot of extra buffer time so you can help recover your own disrupted supply chains and thus sustain a broader recovery effort.

Fourth, focus on the process. To buy time and ensure COTE, critical function providers both public and private require a process that ensures they regularly; (a) map their supporting ecosystem of dependencies, (b) share communication and recovery plans with that ecosystem to empower those agents to proactively assist in recovery, and (c) prepare workarounds and stockpiles adequate to buffer their operations against disrupted support services until recovery of those services can be completed. Several such processes are already practiced by some communities, for example the FEMA five-year planning process[38], or such as the FEMA Community Disaster Resilience Zone planning and certification process[39]. The COTE planning process must be regularized and coordinated with existing business continuity and emergency management processes. A community-based process has advantages over a "stovepiped" sector-specific process because it brings together all critical organizations in an area to coordinate a shared conversation and to share data across layers and functions of the economy. In the USA the appropriate scale for a community COTE process might be the county because FEMA and its state partners implement emergency management functions at the county scale, especially in rural and suburban areas. Major cities may have the resources to execute this process at a finer scale. To expedite the process, training on a standardized participatory framework and use of standardized supply chain and critical infrastructure mapping datasets and analysis tools are both very helpful investments. It is recommended that FEMA or another agency make these standard trainings and tools available free of charge in the near future.

In summary, COTE requires that all critical function providers public or private buy time for recovery through a combination of network dependency mapping, recovery plan communication with upstream and downstream partners, stockpiling of adequate upstream inventory, and establishment of inside-out self-recovery capacity.

4. The Government's Role in Continuity of the Economy

Why is it so important that EM, DHS, and DoD receive supply chain support from the private economy, and why is COTE so important for the EM or defense mission? To answer this question, it is important to understand that government agencies normally assume continuity of their supply chains and supporting infrastructures in support of their critical functions. In other words, the government's emergency responders are assuming an outside-in recovery strategy where emergency responders outside the disaster area surge to support the affected area while supported by an uninterrupted supply chain. This is a realistic assumption when disruptions are localized in nature e.g. an earthquake or severe storm. But this assumption is not correct for systemic cyber threats, an EMP blast, or widespread cascading failures, or for any number of other Black Swan events. Government emergency response capacities are significant when brought to bear on a localized emergency using the outside-in recovery strategy, but when widespread disruptions occur, the capacity of these responders is vanishingly inadequate. Government needs to implement a whole-of-economy COTE strategy so the much larger private sector is prepared to assist with recovery of critical functions when government assets are inadequate.

The limited resources of the government's emergency responders are ideally employed using one of two "force multiplier" strategies: (1) outside-in recovery, and (2) inside-out confrontation. The outside-in

[38] Department of Homeland Security (2016), National Planning System, February 2016.
[39] S.3875 - 117th Congress (2021-2022): Community Disaster Resilience Zones Act of 2022. (2022, December 20). https://www.congress.gov/bill/117th-congress/senate-bill/3875

recovery strategy deals with a major disaster in one geographical area by staging recovery assets from unaffected nearby areas and surging them into the affected area. The inside-out confrontation strategy deals with a threat originating from outside the government's borders by staging defense assets at the border and then thrusting outward to confront the threat. Both of these force multipliers assume the availability of a fully functioning private sector economy in the staging area to supply the logistics and infrastructures required by the EM and defense assets. Without maintaining COTE in that base, the EM and defense assets cannot perform their critical functions for long or at scale. Therefore, in the unfortunate scenario of (3) inside-out recovery from a widespread disruption, where COTE is compromised, the emergency response and recovery assets must assign the highest priority to "jump-starting" their own supporting supply chains and critical infrastructures. This job is much easier if those supporting systems have been prepared ahead of time to independently self-recover. Without quickly re-establishing COTE after a major disruption, the emergency response mission will quickly fail in the inside-out recovery scenario via a negative feedback loop, leading to collapse of the emergency response system and crippling the ability of the broader economy to recover. Roughly 98% of the logistical capacity to respond quickly to a disaster lies in the private sector, not with the government, and this percentage increases to 100% over the medium to long term as prepositioned government resources are exhausted. It becomes clear that the best use of government EM response and recovery resources (1-2% of capacity) will normally be to support private sector organizations which have much greater capacity (98-99% of capacity) to sustain, recover, and enable critical functions. COTE planning creates a "force multiplier" of roughly 50x for government emergency response assets. This force multiplier benefits recovery operations during all kinds of disasters, not only

COTE also increases the efficiency of recovery and response operations by leveraging the much greater expertise and initiative brought to bear by millions of private organizations. The government's emergency response agencies lack the key tactical information and expertise needed to pivot and respond to the millions of different types of supply chain disruptions at a tactical level during a crisis. On the other hand, we know that the millions of private-sector supply chain operators are excellent at taking this initiative during a crisis, having performed admirably in this pivot during the shock of the COVID-19 pandemic[40]. The distributed whole-of-economy approach to recovery has the potential to dramatically outperform the top-down approach during a widespread disruption.

In summary, government emergency response and recovery authorities should focus their efforts on incenting, mandating, training, and providing tools to support whole-of-economy COTE planning, and on supporting recovery of their own supply chains, to be most prepared to handle a widespread disruption.

5. F4R™, A Participatory Process for Planning Continuity of the Economy

The Department of Homeland Security released its "Community Lifelines" approach to supply chain resilience in 2019[41] for the purpose of guiding emergency managers on, *"... how to analyze supply chains and to work with the private sector to enhance supply chain resilience in support of Comprehensive Preparedness Guide 101: Developing and Maintaining Emergency Operations Plans."*[42] Community lifelines are similar to critical infrastructures, and include Safety and Security, Food, Water, Sheltering, Health and Medical, Energy (Power & Fuel), Communications, Transportation, and Hazardous Material.

[40] Sevigny, M. (2020), NAU Research Shows U.S. Supply Chains Still Intact In Midst of Coronavirus. KNAU, March 31st, 2020. Accessed May 10th, 2023 at: https://www.knau.org/knau-and-arizona-news/2020-03-31/nau-research-shows-u-s-supply-chains-still-intact-in-midst-of-coronavirus

[41] DHS, Supply Chain Resilience Guide, April 2019, Washington, DC.

[42] FEMA, *CPG 101: Developing and Maintaining Emergency Operations Plans, Version 2.0,* (Washington, DC, 2010), https://www.fema.gov/media-library/assets/documents/25975.

This DHS guide recommends emergency managers engage in a planning process that maps the supply chains supporting community lifelines and establishes relationships and communications with the people and organizations involved in those supply chains. The DHS guide recommends communities engage in the Regional Resiliency Assessment Program (RRAP) and FEMA's Technical Assistance Program to obtain training and support for the process. These recommendations are conveniently implemented through a COTE process. Fortunately, training, data, and tools are now available to streamline the Community Lifelines and COTE processes in a community.

A current example of a COTE training and planning process is the FEWSION for Community Resilience Network (F4R™, F4R Network™). F4R™ was founded in 2017 through a grant from the National Science Foundation to Northern Arizona University for the purpose of providing US communities with access to the supply chain data science capabilities of the FEWSION research project (https://fewsion.us). The FEWSION project provides the first publicly accessible supply chain datasets and analysis tools for US communities, including the FEW-View™ data visualization engine and the F4R Process™ for applying that data to a community's COTE planning. Figure 4 illustrates the supply chains flowing through Los Angeles to the rest of the world using an infographic developed for FEMA and the County of Los Angeles in 2019 in support of the ShakeOut Exercise. A screenshot of the underlying FEW-View™ [43] source dataset is also included in Figure 4. This data product is now available for every community in the USA at the click of a button. The F4R™ Process is designed for enhanced accessibility to enable small and medium-size communities, rural areas, Tribal communities, and territories to complete a COTE planning process without requiring the specialized expertise and resources available to the largest cities and companies.

The F4R™ process trains participants on the fundamentals of supply chain and resilience theory, and then leads participants through a structured process of data collection, relationship building, and vulnerability analysis implementing the recommendations of the DHS Supply Chain Resilience Guide (Figure 5). At the end of the process the participant will have completed a written report containing the information necessary to satisfy the supply chain resilience and COTE components of their organization's emergency management or business continuity planning process. The F4R Process[44] is well-suited to support FEMA's county-level five-year planning process, in addition to RRAP and Technical Assistance Program activities. F4R currently offers the process to students both as a for-credit college course and as a not-for-credit online continuing education certification, in addition to offering a summer workshop that trains and certifies instructors and facilitators to offer the F4R process in their own communities. Both the online certification and the summer training workshop will equip an emergency manager or resilience professional to implement COTE and Supply Chain Resilience processes in their community. Table 4 summarizes some of the steps involved in the F4R™ Process for COTE.

Most importantly, F4R™ provides a structured process for a peer-to-peer conversation between the private and public stakeholders and participants in the supply chain network. The key to resilience is not a static "plan", but rather the creation of an ongoing disciplined conversation across the network for the purpose of ensuring resilience and COTE. The creation and regular maintenance of this social network is the key to the F4R™ process. At the moment of a major "Black Swan" disruption the COTE planning will "fly out the window", and those relationships and communications will provide the recovery infrastructure we need.

---

[43] Ruddell, B.L., Miller, J., Rushforth, R.R., Salla, R., Soktoeva, E., and Gorantla, R. (2020), 'FEW-View™ 1.2, the FEWSION™ Visualization System', https://fewsion.us and https://fewsion.us/few-view-3/, 02 March, 2020.

[44] Ruddell, B.L., R.R. Rushforth, and S.M. Ryan, F4R™: FEWSION for Community Resilience™ Curriculum, July 16th, 2021 Edition, LuLu Press. https://www.lulu.com/en/us/shop/sean-ryan-and-richard-rushforth-and-benjamin-ruddell/f4rtm-fewsion-for-community-resiliencetm-curriculum/hardcover/product-eqndpg.html?page=1&pageSize=4

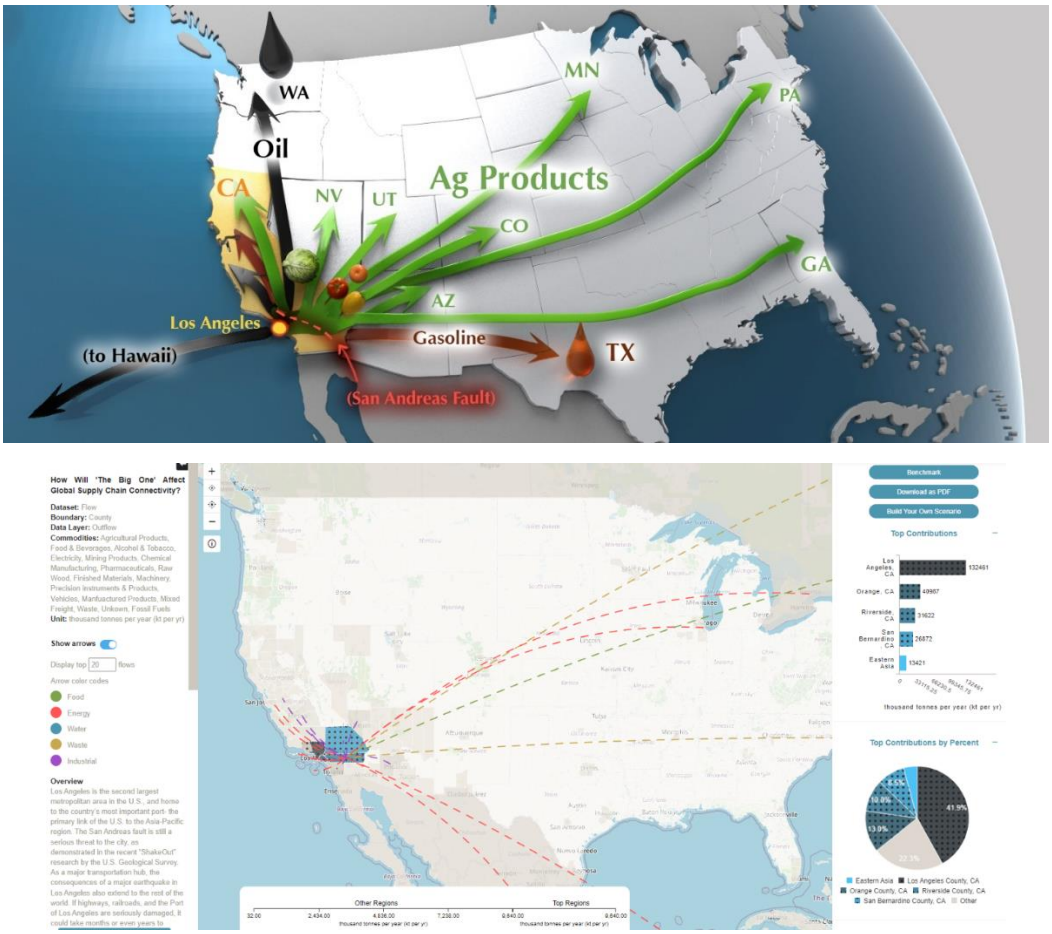

Figure 4: Global supply chains flowing through the LA Metropolitan Area in support of the FEMA and County of Los Angeles ShakeOut exercises in 2019; (top) infographic, and (bottom) screenshot of the supply chain data visualized using FEW-View™. Critical infrastructures and supply chains around the world will be compromised by a major LA earthquake.

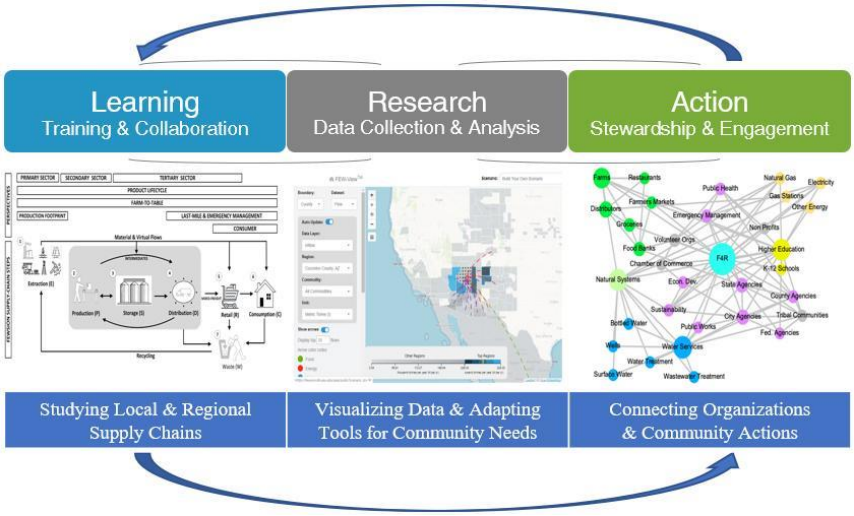

Figure 5. FEWSION for Community Resilience (F4R) is an iterative participatory process that leverages supply chain data science to build systems thinking and systems management capacity in local communities through three key activity types: Learning, Research, and Action.

Table 4: Summary of the three phases and main steps in the F4R™ process for COTE planning.

Phase 1: Learning
Learn systems thinking concepts
Learn resilience concepts and measurements
Learn the structure of the economy and supply chains
Learn how to use supply chain and critical infrastructure data and tools
Learn a structured process for COTE planning
Phase 2: Research
Critical Infrastructure mapping
Social Network and Contact mapping
Supply Chain mapping
Threat mapping
Phase 3: Action
Align the COTE process with other regulatory and planning process
Convene a stakeholder conversation
Connect supply chain suppliers and dependents
Develop proactive mitigation priorities to boost resilience
Initiate funding and authorization for mitigation priorities
Compile and distribute COTE recovery plans to stakeholders

INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Ruddell, B. L. (2023) Rationale and Process for Continuity of the Economy. (Report No. IHS/CR-2023-1021). The Sam Houston State University Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/87ESH