Governing Cascade Failures in Complex Social-Ecological-Technological Systems: Framing Context, Strategies, and Challenges

J.B. Ruhl[*]

ABSTRACT

Cascade failures are events in networked systems with interconnected components in which failure of one or a few parts triggers the failure of other parts, which triggers the failure of more parts, and so on. Cascade failures occur in a wide variety of familiar systems, such as electric power distribution grids, transportation systems, financial systems, and ecosystems. Cascade failures have plagued society for centuries. However, modern social-ecological-technological systems (SETS) have become vast, fast moving, and highly interconnected, exposing these systems to cascade failures of potentially global proportions, spreading at breathtaking speed, and imposing catastrophic harms. The increasing potential for cascade failures of the magnitude of the 2008 financial system collapse, which had a truly global reach and affected systems well beyond finance, screams out for clear thinking about governing vulnerability to cascade failures in SETS. Yet, legal scholarship on the theme is essentially nil, and a more comprehensive, generalizable governance theory leveraging knowledge from scientific research on cascade failures has not emerged. Research initiatives are needed to forge ground on three fronts: (1) system modeling and monitoring; (2) event prediction; and (3) event prevention,

---

[*] David Daniels Allen Distinguished Chair of Law, Vanderbilt University Law School. I am immensely grateful to the *Vanderbilt Journal of Entertainment & Technology Law* for inviting me to participate in the symposium on "Regulating the Unregulatable" and for the editing support they provided for this written version of my presentation on cascade failures. I also benefitted immeasurably from the comments on an early draft I received at the second annual Southern Environmental Law Scholars Workshop from Nadia Ahmad, Nick Bryner, Josh Eagle, Sharon Jacobs, Jonas Monast, Jonathan Nash, Jessie Owley, Gabe Pacyniak, Nathan Richardson, Kalyani Robbins, Amy Stein, Mike Vandenbergh, and Shelley Welton, and I am grateful to the law schools at the University of Florida, the University of South Carolina, and Vanderbilt University for providing funding support for the workshop.

response, and recovery. This Article is a first step in that direction. Part I outlines the cascade failures problem. Part II summarizes the scientific research on cascade failures. Part III identifies strategies for controlling cascade failures. Part IV explores the governance challenges of deploying those various strategies in large-scale SETS. Part V extends the analysis to the special case of cascade failures within ecological systems and the difficulties of managing them through the strategies coming out of cascade failures science. Lastly, Part VI suggests directions of future research on governance of cascade failures.

TABLE OF CONTENTS

I. INTRODUCTION

On May 7, 2019, unknown criminals from an unknown location took control of most of the city of Baltimore's municipal online computer servers, freezing all access to them, and demanded a ransom payment of $80,000 in Bitcoin within ten days or else all of the city's data would be destroyed.[1] Having pursued an agenda of moving many municipal

1. The events recounted in this paragraph are documented with references to sources at *A Timeline of the Baltimore City Ransomware Attack*, CYWARE, https://cyware.com/blog/a-timeline-

services and payment systems from paper to online, the effects of the attack rippled through Baltimore's public and private sectors. City employees, who had no access to their work computers and email accounts, opened Gmail accounts on their personal computers, but Google flagged the bulk creation of accounts from the same network as suspicious and automatically froze them (though they were restored soon after). Property sales could not go forward without information from the city's online system, and property tax, water bills, parking tickets, and many other forms of payments to the city could not be completed. The city migrated many functions back to paper, but the wheels of city services then moved slowly. By the end of the month, Baltimore officials estimated the cost of restoring all systems to be over $18 million. Apparently frustrated by the city's refusal to pay the ransom, in early June, the attackers began releasing sensitive documents and threatened to leak citizens' personal information on the dark web. One month after the attack, just over a third of city employees had access to their computers and email accounts. By mid-June, most employees were back online, but many payment systems were still offline and far behind—for example, the city warned that water meters would continue to read water use while the payment system is offline, so residents should expect unusually high water bills once that system recovered.

In short, Baltimore experienced a cascade failure.[2] Cascade failures are events in networked systems with interconnected components in which failure of one or a few parts triggers the failure of other parts, which triggers the failure of more parts, and so on.[3] Cascade failures are found in a wide variety of familiar systems, such as electric power distribution grids, transportation systems, financial systems, and ecosystems.[4] The financial crisis of 2008 has been

---

of-the-baltimore-city-ransomware-attack-d006 [https://perma.cc/X43Y-D432] (last updated June 5, 2019).

2. Baltimore is by no means alone in experiencing this form of ransomware. *See* Manny Fernandez, David E. Sanger & Marina Trahan Martinez, *Ransomware Attacks Are Testing Resolve of Cities Across America*, N.Y. TIMES (Aug. 22, 2019), https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html [https://perma.cc/CCC2-PKTV]; Frances Robles, *A City Paid a Hefty Ransom to Hackers. But Its Pains Are Far from Over*, N.Y. TIMES (July 7, 2019), https://www.nytimes.com/2019/07/07/us/florida-ransom-hack.html [https://perma.cc/A9ZQ-U79R].

3. Raissa M. D'Souza, *Curtailing Cascading Failures*, 358 SCIENCE 860, 860 (2017); Yang Yang et al., *Small Vulnerable Sets Determine Large Network Cascades in Power Grids*, 358 SCIENCE 886, 886 (2017).

4. Qian Zhu et al., *Optimization of Cascading Failure on Complex Network Based on NNIA*, 501 PHYSICA A 42, 42 (2018); D'Souza, *supra* note 3; John W. Terborgh, *Toward a Trophic Theory of Species Diversity*, 112 PROC. NAT'L ACAD. SCIS. 11415 (2015).

described as a cascade failure,[5] and the loss of "keystone" species in an ecosystem can lead to cascading effects throughout the ecosystem.[6] In these and many other cases, the failure of one system component is all it takes to trigger the cascade failure, as in the case of the Lehman Brothers bankruptcy.[7] The cause of the initial failure event can seem random and trivial in isolation,[8] and the same event in the same system will not always trigger a cascade failure.[9] Once the cascade starts, however, it can be virtually unstoppable.[10] Failure in one system can also jump to other interconnected systems as well—for example, a power station failure could knock out a regional distribution grid, which then shuts down water supply systems, which then disrupts wastewater treatment plants, and so on.[11]

Although it can be easy to imagine how cascade failures like this could happen, researchers have not made much progress on predicting when, where, how, and why they happen, and even less progress has been made on what to do about a cascade failure when it does happen. Some systems, particularly those with complex interconnections, are believed to build up greater "systemic risk" exposure to cascade failures,[12] but beyond that core principle, researchers are still continuing to explore questions about the conditions of systemic risk, how failure moves through the system, how systems repair after failure, and other basic properties of cascade failure.[13]

Cascade failures have plagued society for centuries. However, modern social and technological systems have become vast, fast moving, and highly interconnected, exposing these systems to cascade failures of potentially global proportions, spreading at breathtaking speed, and imposing catastrophic harms. The chief driver behind this quantum shift in failure speed and magnitude has been advancements in technology, specifically (1) the expanding reach and connections to the internet;[14] (2) the ever-larger and more interconnected infrastructure

5. FIN. CRISIS INQUIRY COMM'N, THE FINANCIAL CRISIS INQUIRY REPORT 432 (2011) (assessing causes of the financial crisis, including failures in regulation).

6. Terborgh, *supra* note 4.

7. FIN. CRISIS INQUIRY COMM'N, *supra* note 5, at xvi, 324.

8. D'Souza, *supra* note 3, at 861.

9. *Id.*

10. *Id.*

11. COMM'N TO ASSESS THE THREAT TO THE U.S. FROM ELECTROMAGNETIC PULSE (EMP) ATTACK, CRITICAL NATIONAL INFRASTRUCTURES 34, 142 (Apr. 2008).

12. Yang et al., *supra* note 3.

13. *Id.*

14. Zhu et al., *supra* note 4.

systems;[15] and (3) vast increases in computational capacity and speed, allowing rapid automation of system operations and decisions.[16] Today, there exists a globally connected society in which information travels around the world in a matter of seconds and people, energy, goods, and materials can move around in increasingly larger quantities, at faster speeds, and over greater distances. Technology more generally has also been the driver of increasingly frequent and larger ecological cascade failures, such as climate change[17] and loss of biodiversity.[18] Indeed, although we often compartmentalize social, ecological, and technological systems as distinct, it is becoming difficult to disaggregate them in operation, as automated online systems increasingly run infrastructure systems, expanding infrastructure systems increasingly degrade ecological systems, and degraded ecological systems diminish the resilience of human social and economic systems.[19]

Researchers have begun referring to and studying these vast "systems-of-systems" as complex social-ecological-technological systems (SETS).[20] As one researcher explains:

> Adopting a SETS lens can help identify vulnerabilities that develop within infrastructure systems over time. Ultimately, adopting this SETS perspective will

15. COMM'N TO ASSESS THE THREAT TO THE U.S. FROM ELECTROMAGNETIC PULSE (EMP) ATTACK, *supra* note 11, at 1, 18, 92, 134, 143.

16. Patrick McCarthy, *Infographic: The Growth of Computer Processing Power*, RECOIL OFFGRID (May 2, 2017), https://www.offgridweb.com/preparation/infographic-the-growth-of-computer-processing-power/ [https://perma.cc/S7Z5-7KDU]; *see also* Jin Yoshikawa, *Sharing the Costs of Artificial Intelligence: Universal No-Fault Social Insurance for Personal Injuries*, 21 VAND. J. ENT. & TECH. 1155, 1159–60 (2019).

17. IPCC, GLOBAL WARMING AT 1.5°C 6, 26 (2018).

18. INTERGOVERNMENTAL SCI.-POLICY PLATFORM ON BIODIVERSITY & ECOSYS. SERVS., SUMMARY FOR POLICYMAKERS OF THE GLOBAL ASSESSMENT REPORT ON BIODIVERSITY AND ECOSYSTEM SERVICES OF THE INTERGOVERNMENTAL SCIENCE-POLICY PLATFORM ON BIODIVERSITY AND ECOSYSTEM SERVICES 3 (2019).

19. Samuel A. Markolf et al., *Interdependent Infrastructure as Linked Social, Ecological, and Technological Systems (SETSs) to Address Lock-in and Enhance Resilience*, 6 EARTH'S FUTURE 1638, 1638 (2018); COMM'N TO ASSESS THE THREAT TO THE U.S. FROM ELECTROMAGNETIC PULSE (EMP) ATTACK, *supra* note 11, at 34.

20. Samuel A. Markolf et al., *supra* note 19; Nancy B. Grimm et al., *Does the Ecological Concept of Disturbance Have Utility in Urban Social-Ecological-Technological Systems?*, 3 ECOSYS. HEALTH & SUSTAINABILITY 1, 1 (2017); John C. Little et al., *A Tiered, System-of-Systems Modelling Framework for Resolving Complex Socio-Environmental Policy Issues*, 112 ENVTL. MODELLING & SOFTWARE 82, 82 (2019). The SETS model has emerged from the broad research agenda focused on management of social-ecological systems. *See* Maja Schlüter et al., *Capturing Emergent Phenomena in Social-Ecological Systems: An Analytical Framework*, 24 ECOLOGY & SOC'Y art. 11 (2019), https://www.ecologyandsociety.org/vol24/iss3/art11/ [https://perma.cc/KRX4-ERPV]. Under some conditions—e.g., management of a lake in a rural area—technological systems might not play an important direct role in system dynamics. This is decreasingly the case, however, as climate change—the product primarily of technological systems—is affecting ecological and social systems globally.

> not only help us better understand our infrastructure systems, but also aid in the development strategies for adapting to the many challenges that our infrastructure will continue to face (climate change, interdependencies, technological evolution, growing complexity, etc.).[21]

As social, ecological, and technological systems increasingly become interconnected at larger scales into SETS, they become inseparable, and tinkering in one subsystem can affect multiple other interconnected subsystems.[22] Consider communication of information between people. Long ago, of course, it was all by word of mouth. That was a purely social system. But successive technological advancements—writing, the printing press, the telegraph, the telephone, and so on until today's internet—have leveraged technological networks to vastly increase the speed and scale of human communications embedded in technological infrastructure. Are Facebook and Twitter social systems or technological systems? They are both—one does not exist without the other.

To be sure, plenty of social benefits are made possible by the scale and power of this new breed of massive systems-of-systems—no one is proposing to do away with the internet—but part of what is made possible is also system-wide failure. As one study on infrastructure explained:

> The physical and social fabric of the United States is sustained by a system of systems; a complex and dynamic network of interlocking and interdependent infrastructures ("critical national infrastructures") whose harmonious functioning enables the myriad actions, transactions, and information flow that undergird the orderly conduct of civil society in this country. The vulnerability of these infrastructures to threats—deliberate, accidental, and acts of nature—is the focus of greatly heightened concern in the current era, a process accelerated by the events of 9/11 and recent hurricanes, including Katrina and Rita.[23]

The increasing potential for cascade failures of the magnitude of the 2008 financial system collapse, which had a truly global reach and affected systems well beyond finance,[24] screams out for clear thinking about governing vulnerability to cascade failures in SETS. Much like the governance of natural disasters, such as wildfires and hurricanes,[25] and of emergencies more generally,[26] cascade failure governance would involve improvements in system monitoring, event prediction, and

---

21. Markolf et al., *supra* note 19.

22. *Id.*

23. COMM'N TO ASSESS THE THREAT TO THE U.S. FROM ELECTROMAGNETIC PULSE (EMP) ATTACK, *supra* note 11, at vi.

24. FIN. CRISIS INQUIRY COMM'N, *supra* note 5.

25. *See* DANIEL A. FARBER ET AL., DISASTER LAW AND POLICY (3rd ed. 2015).

26. *See* Amy L. Stein, Delegating Emergency Powers 28 (Aug. 16, 2019) (unpublished draft) (on file with author).

harm prevention, response, and recovery. Although governance scholarship has touched on some of these qualities in various settings, particularly through studies of systemic risk in financial systems,[27] electric power grids,[28] and ecological systems,[29] legal scholarship on the theme is essentially nil,[30] and a more comprehensive, generalizable governance theory leveraging knowledge from scientific research on cascade failures has not emerged. This Article is a first step in that direction.

The Article proceeds in five parts. Part II provides a background on the current science of cascade failures, which focuses primarily on technological systems such as power grids and the financial systems, describing what is known about them and what remains to be explored and answered (the latter being by far the larger category). Part III contextualizes that background in the domain of SETS governance, outlining possible public and private measures that could extend strategies being developed in the technological applications into social and ecological settings, such as finance, social media, and climate change. Part IV explores the governance challenges of deploying those various strategies in large-scale SETS, particularly given that some strategies, such as walling off vulnerable system components or cutting off connections to block a cascade, can impose serious harm to some parts of a system in order to prevent more widespread harm throughout the system. Part V extends the analysis to the special case of cascade failures within ecological systems and the difficulties of managing them through the strategies coming out of cascade failures science. Part VI concludes with some thoughts about the directions of future research on governance of cascade failures, particularly those looming large on the horizon as technology advances.

The Baltimore ransomware debacle, and its severe consequences to the city and its citizens, both could have been prevented and could have been much worse. Information technology experts have criticized

27. Stefano Battiston et al., *Complexity Theory and Financial Regulation*, 351 SCIENCE 818, 818 (Feb. 19, 2016); Caitlin Chambers et al., *The System Made Me Do It? Regulating Systematic Risk*, *in* GLOBAL CHALLENGES, GOVERNANCE, AND COMPLEXITY: APPLICATIONS AND FRONTIERS 212–239 (Victor Galaz ed., 2019).

28. Massoud Amin, *Challenges in Reliability, Security, Efficiency, and Resilience of Energy Infrastructure: Toward Smart Self-Healing Electric Power Grid*, IEEE (2008), https://iee-explore.ieee.org/abstract/document/4596791 [https://perma.cc/7T89-EK86].

29. Marten Scheffer et al., *Catastrophic Shifts in Ecosystems*, 413 NATURE 591, 591 (2001).

30. A Westlaw search conducted on June 22, 2019, in the Law Reviews and Journals library for "cascade failure" resulted in seven articles, none of which discuss the theme comprehensively.

the city for failing to keep up with cyberattack prevention measures.[31] That was a governance failure. Luckily, however, Baltimore was for all practical purposes an island—the attack did not spread to other jurisdictions' systems because its system was not connected to them. Connections between systems can add to overall efficiency and robustness of the "system-of-systems" but also open the door to broader harm when one system suffers a failure that spreads to other systems. As global society increasingly reaps the benefits of larger, faster, more connected systems embedded in SETS, cascade failure in SETS looms larger as a governance challenge.

II. THE SCIENCE OF CASCADE FAILURES

Wherever you are the moment you are reading this sentence, pause for a moment and look around you. Chances are you are benefitting from many different systems—the electric power grid is delivering energy for lights, computers, and ventilation systems; the internet is allowing you access to email, entertainment, and information; and telecommunications systems allow you to call a friend. Later today, you may use a credit card (financial system) to buy a meal at a grocery store (food system) on your way home via light-rail (transportation system). Very few people know in detail how any one of these systems works, and almost nobody knows how all of them work. Now imagine that they all fail—the lights go off, computers shut down, and ventilation stops; your phone doesn't work; the store has no food, but your credit card doesn't work anyway; the trains stop running. Obviously, something went wrong. But what, and why?

This scenario is not outlandish. For example, a massive electromagnetic pulse, whether from a high-altitude nuclear detonation or a massive solar-flare storm, has the potential to disrupt the nation's entire electric power distribution grid, in which case every inconvenience described in the scenario, and more, will happen as the lack of power spreads through and disables other interconnected infrastructure components (illustrated in Figure 1).[32] Indeed, a brief

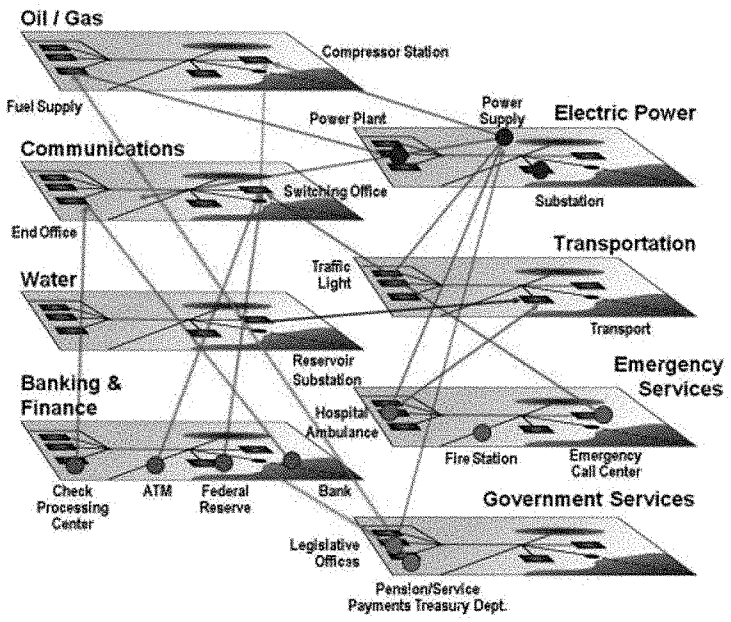
---

31. Dave Weinstein, *Hackers Hold Baltimore Hostage*, WALL ST. J. (May 30, 2019, 6:52 PM), https://www.wsj.com/articles/hackers-hold-baltimore-hostage-11559256722 [https://perma.cc/D9UU-MUKU].

32. COMM'N TO ASSESS THE THREAT TO THE U.S. FROM ELECTROMAGNETIC PULSE (EMP) ATTACK, *supra* note 11, at 160; COMM'N TO ASSESS THE THREAT TO THE U.S. FROM ELECTROMAGNETIC PULSE (EMP) ATTACK, EXECUTIVE REPORT 1 (July 2017), http://www.firstemp-commission.org/uploads/1/1/9/5/119571849/executive_report_on_assessing_the_threat_from_emp_-_final_april2018.pdf [https://perma.cc/62TS-Z28B]; Sarah Scoles, *The Calm Before the Storms*, SCIENCE 818, 818–19 (May 31, 2019) ("[Solar] storms can disrupt communications, interrupt spacecraft and missile tracking, and skew GPS measurements. They

taste of that possibility occurred in June 2019, as the failure of one generating unit of the power system in Argentina shut down power throughout that nation and parts of four others for the better part of a day.[33] And the Baltimore experience demonstrates the far-reaching impact of just one system—in that case, a few computer system servers—failing.

Figure 1. A Conceptual Illustration of the Interconnectedness of Elements Contained Within Each Critical Infrastructure[34]



Cascade failures like these are network phenomena.[35] Networks consist of components ("nodes") connected by some form of flow channels ("edges" or "links") that move information, energy, money, or whatever else the network distributes between the components.[36] Some

can also induce powerful currents in electric grids, which can destroy transformers and other equipment.").

33. Daniel Politi & Clifford Krauss, *'Massive Failure' in Power Grid Causes Blackout in Argentina and Uruguay*, N.Y. TIMES (June 16, 2019), https://www.nytimes.com/2019/06/16/world/americas/power-outage-argentina-uruguay.html [https://perma.cc/FT9T-P79J].

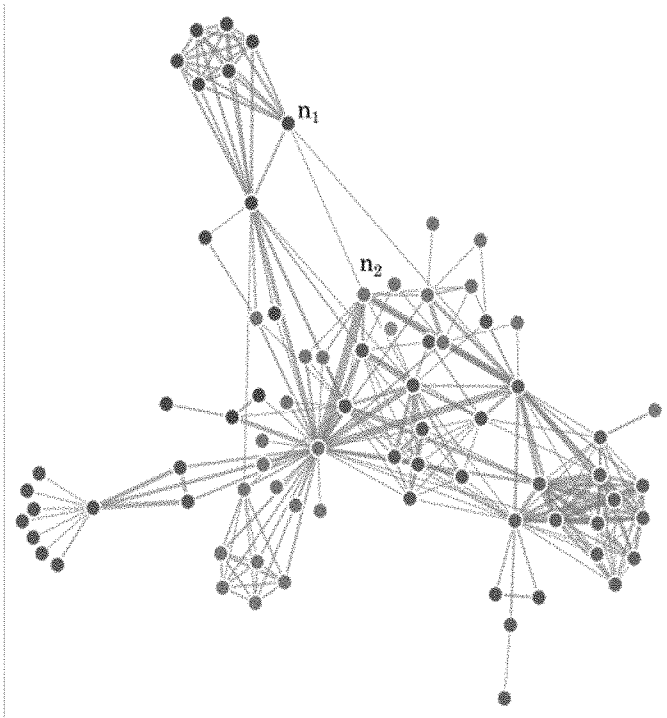
34. COMM'N TO ASSESS THE THREAT TO THE U.S. FROM ELECTROMAGNETIC PULSE (EMP) ATTACK, *supra* note 11, at 12.

35. Junbiao Liu et al., *Threshold for the Outbreak of Cascading Failures in Degree-Degree Uncorrelated Networks*, 2015 MATHEMATICAL PROBS. ENGINEERING, at 1, http://dx.doi.org/10.1155/2015/752893 [https://perma.cc/N64M-6BYR].

36. MATTHEW O. JACKSON, SOCIAL AND ECONOMIC NETWORKS 3–43 (2008).

nodes have a greater number of connections ("degree") than others.[37] Figure 2 depicts a hypothetical network of different types of nodes (arranged in loose clusters) connected by links within and across node types, with nodes having varying degrees.

Figure 2. Network Graph Diagram Showing Nodes of Different Types, Links, and Degrees[38]



Network researchers have developed an array of metrics and properties for describing network structure and behavior.[39] This Part of the Article focuses on three network properties relevant to governance of cascade failures: (1) systemic risk, (2) failure propagation, and (3) network resilience.

37. *Id.*

38. This network diagram is a famous graph by Mike Bostock of the character co-occurrence in the book *Les Misérables*. *See* Mike Bostock, *Les Misérables Co-occurrence*, BOST.OCKS.ORG (Apr. 10, 2012), https://bost.ocks.org/mike/miserables/ [https://perma.cc/35MP-NF32]. This version is from Observable. *See* Mike Bostock, *Force-Directed Graph*, OBSERVABLE (Nov. 15, 2017), https://observablehq.com/@d3/force-directed-graph [https://perma.cc/6MHX-WYCC]. But it could be a graph of any number of other kinds of networks.

39. *See* Bostock, *Les Misérables Co-occurrence*, *supra* note 38; Bostock, *Force-Directed Graph*, *supra* note 38.

A. Systemic Risk

Network researchers have begun to identify some attributes of network structure and node connectivity that help explain the conditions under which systemic risk of cascade failure is high. The unifying research question is posed as: Under what conditions would an initial disturbance remain localized rather than cascade through the network?[40] At one extreme, a node that is not connected to the network can fail and have no cascade effects because there is no means for the failure's effects to enter the network. At the other extreme, a node that is connected can fail and the entire network collapses. Research on paradigmatic networks, such as power grids and banking systems, as well as in simulation models, suggests that networks at that end of the spectrum tend to exhibit coupled subnetworks with high interdependency (e.g., the national power grid is a network of smaller regional grids). A node connects to such a network to function, but it may not matter through which path of links and nodes it receives its supply of the functional medium (money, information, energy, etc.).

If it does matter, however—if a node must receive a critical supply of network flow from another specific node—then the node necessarily becomes dependent on all the other nodes along its critical pathway of links. And if those pathways travel through more than one subsystem in the giant network, those subsystems become interdependent as well. Indeed, a node in one subsystem might be more dependent on a node in another subsystem than it is on any node in its own subsystem.[41] Those two nodes could also connect via a "shortcut" link that involves no other nodes in either system, allowing direct channeling of the network flow between subsystems.[42] For example, in Figure 2, a node near the top, n_1, has a shortcut link to a node in the center right, n_2, which could allow network flow to move directly between their respective clusters rather than through a longer multinode pathway.

The kind of system-of-systems described here is different in structure from a simple isolated network in which all nodes and links are uniform throughout the system.[43] Complex networks exhibit more heterogeneity, with clusters of tightly connected nodes, nodes having varying degrees of connections, and some nodes serving as shortcuts to

40. Yang et al., *supra* note 3.

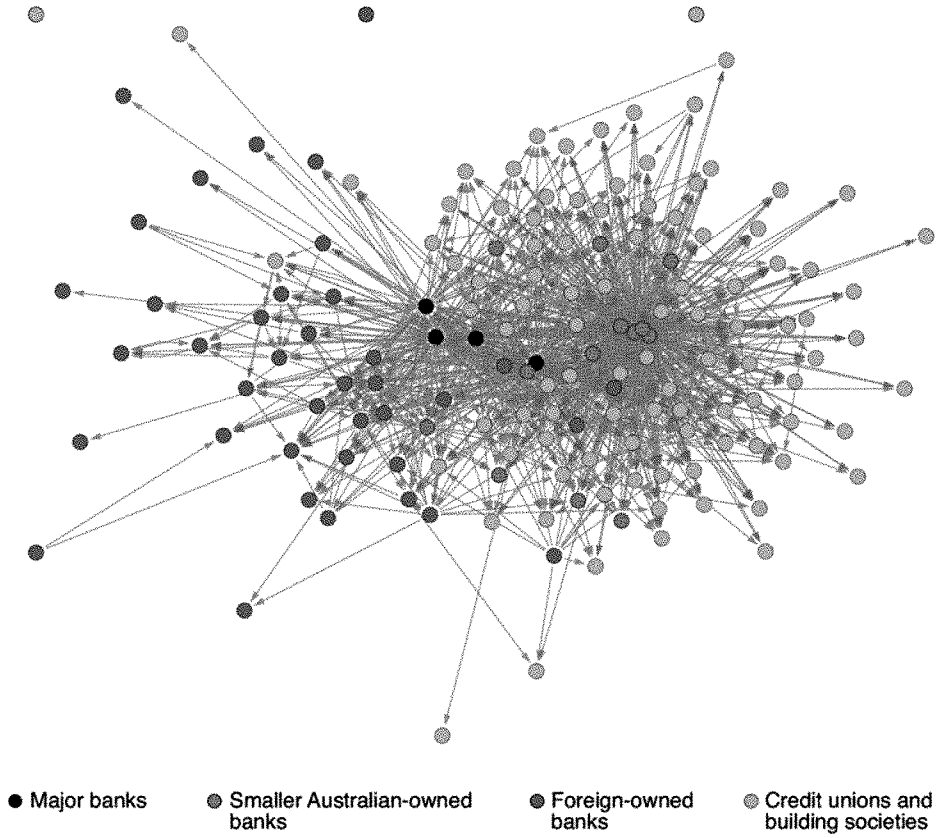
41. Sergey V. Buldyrev et al., *Catastrophic Cascade of Failures in Interdependent Networks*, 464 NATURE 1025, 1025 (Apr. 15, 2010).

42. Arun Kumar et al., Pro*tection Strategies Against Cascading Failure for Power Systems of Ring Network*, 8 COMM. & NETWORK 67, 68 (May 12, 2016).

43. Yang et al., *supra* note 3.

other subsystems. For example, Figure 3 shows the structure of the Australian banking system with different types of banks and links showing loan exposures between borrowers and lenders (arrows flow from borrower to lender). Banks near the center of the network have high degrees of exposure. Banks on the edges have less exposure, and some have none.

Figure 3. Australian Banking System Network of Large Exposure[44]



44. Eduardo Tellez, *Mapping the Australian Banking System Network*, RES. BANK AUSTL. BULL. 45, 49 (June 2013), https://www.rba.gov.au/publications/bulletin/2013/jun/pdf/bu-0613-6.pdf [https://perma.cc/CD64-MV8F].

While this complexity of structure may make the system more robust at carrying out its functions, it ironically is also the source of systemic risk.[45] As a growing body of research demonstrates:

> [T]he coupling between different networks induces a dynamical process of cascading failures; a failure of nodes in one network leads to a failure of dependent nodes in other networks, which in turn may cause further damage to the first network and so on. This sequence of cascading failures may totally fragment the entire system . . . . [T]he coupling strength of the networks, represented by the fraction q of interdependent nodes, determines the way the system collapses. For strong coupling, that is, for a high fraction of interdependent nodes, an initial damage event can lead to cascading failures that yield an abrupt collapse of the system, in a form of a first-order phase transition. Reducing the coupling strength below a critical value, qc, leads to a change from an abrupt collapse to a continuous decrease of the size of the network.[46]

In systems-of-systems exhibiting high degrees of coupling—i.e., with coupling above the critical value qc—which nodes and which pathways between subsystems matter, and when do they matter? That may depend on variable conditions. In an electric power grid, for example, there may be many cross-system shortcut pathways, and they may change in topology as switching between different nodes (e.g., power supply units) occurs dynamically. Emerging research suggests two properties are of the most concern. First, higher densities of shortcut links between subsystems—the direct connections between two nodes across the subsystems moving critical flow from one to the other (or between both)—are associated with higher systemic risk.[47] Second, there can be a small "vulnerable set" of nodes, the failure of which can trigger system-wide cascades.[48] These nodes tend to be located in areas of the system with high densities of links and concentrated levels of flow load through the system (e.g., densely populated areas of a power service grid).[49] Thus, "the primary failure of a few links within or near a vulnerable set of links causes a disproportionate number of large cascades."[50] In a dynamic system, however, the exact set of vulnerable links can change, but the overall number of vulnerable links is small[51] and can be roughly identified by

45. David L. Alderson & John C. Doyle, *Contrasting Views of Complexity and Their Implications for Network-Centric Infrastructures*, 40 IEEE TRANSACTIONS ON SYS., MAN & CYBERNETICS 839, 843 (2010).

46. Amir Bashan et al., *The Extreme Vulnerability of Interdependent Spatially Embedded Networks*, 9 NATURE PHYSICS 667, 667 (Aug. 25, 2013).

47. Kumar et al., *supra* note 42, at 76–77.

48. D'Souza, *supra* note 3; Yang et al., *supra* note 3.

49. D'Souza, *supra* note 3, at 861; Yang et al., *supra* note 3.

50. D'Souza, *supra* note 3, at 861; Yang et al., *supra* note 3.

51. Buldyrev et al., *supra* note 41; D'Souza, *supra* note 3; Yang et al., *supra* note 3.

their higher level of recurrent failure.[52] Table 1 summarizes what research has suggested are complexity features that increase systemic risk of cascade failure.

Table 1. Features Increasing Systemic Risk to Cascade Failure

Feature	Risk Factor
Subnetworks	Clustering of nodes into multiple subsets increases system complexity
Coupling	Higher interdependency between subnetworks increases chances of failure propagation between subnetworks
Shortcuts	Direct links between subnetworks facilitate failure propagation
Heterogeneity	Variability in nodes and subnetworks increases system complexity
Topology	Dynamic system topology increases system complexity and makes propagation pathway prediction more difficult
Vulnerable sets	Clusters of weak nodes increase the chance of failure events
Density	Density of nodes, particularly around vulnerable sets, increases chances of failure propagation

B. Failure Propagation

As research begins to reveal the conditions under which systemic risk of cascade failure is high and the points at which failure may be triggered, it is equally important to understand how and where failure cascades through the systems-of-systems. Generally, two modes of failure propagation have been identified. In structural failures, damages spread directly, node-by-node, along the node-link pathways that bind the subsystems together, like a chain reaction.[53] A chain reaction is essentially the same event happening over and over, moving through the system in linear node-to-node fashion, like the classic setup

52. Buldyrev et al., *supra* note 41; D'Souza, *supra* note 3, at 861; Yang et al., *supra* note 3.

53. Li Daqing et al., *Spatial Correlation Analysis of Cascading Failures: Congestions and Blackouts*, 4 SCI. REP., June 20, 2014, at 1, https://www.nature.com/articles/srep05381 [https://perma.cc/XX8R-HVC2].

of dominos falling one after the other.[54] By contrast, overload failures occur when the system responds to a perturbation (e.g., a wind storm knocks over a transformer) by rerouting network flow to the point that a node fails and immediately sheds the flow overload to other nodes, some of which fail and shed even more overload into the system.[55] But not every node along the way fails—some manage to move the overload along without failing, and it is a node further along in the chain that next fails. The propagation of overload failure, therefore, is not necessarily a node-by-node line of failure along direct node-link pathways. Rather, a node fails in one network location, then in another potentially distant location, and so on in unpredictable patterns until the overload becomes a global drag on the system as a whole.[56] As a number of network scientists explain, "In marked contrast to cascading structural failures, overload failures usually interact and propagate in networks globally due to cooperative overload pressure, without visible or direct causal relations."[57] This kind of failure-hopping effect has been observed in collapses of power grid systems and banking systems, where primary failure of one set of nodes is followed by failure of another set of nodes located far away in the network from the first set, and so on.[58]

Between the two propagation patterns, overload failures are by far the bigger management and response challenge.[59] Consider again the power grid example. If failure follows a structural node-by-node line pattern, the system manager could cut off a cascade by severing the links located ahead of the failing nodes. In overload failures, however, the system manager cannot necessarily follow the propagation of failure node-by-node.[60] A cluster of nodes could fail in one location, after which the overload would move through the system without failure along many node-link pathways before it would bring down another set of

54. To watch dominos falling for thirty minutes, see Hevesh5, *30 Minutes of DOMINOES FALLING! – Most Satisfying ASMR Compilation*, YOUTUBE (Dec. 15, 2018), https://www.youtube.com/watch?v=bUl295oyeIc [https://perma.cc/U93M-RUAA].

55. Daqing et al., *supra* note 53; Liu et al., *supra* note 35; Hoang Ahn Q. Tran & Akira Namatame, *Improve Network's Robustness Against Cascade with Rewiring*, 24 PROCEDIA COMPUTER SCI. 239, 240 (2013).

56. For a stunning visualization of this effect in the power grid context, see Jun Yan, *Demo of a Potential Cascading Failure in San Francisco Bay Area*, YOUTUBE (Dec. 23, 2014), https://www.youtube.com/watch?v=SGWDBsQNilU [https://perma.cc/S99F-YNTU].

57. Daqing et al., *supra* note 53.

58. D'Souza, *supra* note 3 (power grids); Daqing et al., *supra* note 53 (banking).

59. Daqing et al., *supra* note 53.

60. Xuqing Huang et al., *Cascading Failures in Bi-Partite Graphs: Model for Systemic Risk Propagation*, 3 SCI. REP., Feb. 5, 2013, at 1, https://www.nature.com/articles/srep01219 [https://perma.cc/JB8Y-WQZE].

distant nodes, and so on. To stop the cascade, the system manager may have no option other than shutting down the entire system to cut losses. Indeed, power distribution companies in the western United States, where wildfires have been triggered by the sparks emitted from overload failures (e.g., line failure from wind leads to exploding transformers elsewhere), have begun implementing that approach for system management during high wind and other risk conditions.[61]

C. Network Resilience

Even systems with high levels of systemic risk aren't constantly failing. Not every transformer outage or fender bender brings down the system. Systems can be resilient. The question is how to make them so.

In their deep examination of resilience in complex network systems, Alderson and Doyle explain that five key features of a system contribute to the capacity to endure through surrounding change:

> *Reliability* involves robustness to component failures. *Efficiency* is robustness to resource scarcity. *Scalability* is robustness to changes to the size and complexity of the system as a whole. *Modularity* is robustness to structured component rearrangements. *Evolvability* is robustness of lineages to changes on long time scales.[62]

As they go on to point out, however, as much as these properties build resilience, trade-offs between them can open the door to cascade failure.[63] Consider the shortcut link strategy for moving network flow between two nodes in different subsystems. A shortcut provides efficiency of flow of the network medium (information, money, energy) by providing a direct subsystem-to-subsystem pathway rather than routing the flow along the multinode pathway out of one subsystem and to the other. By providing an expedient route from one subsystem to another, it also sheds overload—and thus risk. However, shortcuts could also impair system resilience when the shortcut becomes a pathway that speeds up failure propagation. On the other hand, boosting modularity (e.g., by adding more variety of components) or scalability (e.g., by continually adding components) could demand resources that drain efficiency, exposing the system to failure if resources become scarce.

---

61. Katherine Blunt, Jim Carlton & Erin Ailworth, *PG&E Starts to Cut Power for Nearly 800,000 California Customers on Wildfire Risk*, WALL ST. J. (Oct. 9, 2019, 5:56 PM), https://www.wsj.com/articles/ pg-e-warns-it-may-cut-power-for-600-000-customers-due-to-wildfire-risk-11570513569 [https://perma.cc/8MM9-YUB8].

62. Alderson & Doyle, *supra* note 45, at 840; *see also* A. Li et al., *The Fundamental Advantages of Temporal Networks*, 358 SCIENCE 1042, 1042 (Nov. 24, 2017); Marta Sales-Pardo, *The Importance of Being Modular*, 357 SCIENCE 128, 128 (July 14, 2017).

63. Alderson & Doyle, *supra* note 45, at 840.

Researchers have focused on how to balance these five properties of resilience in the quest to reduce the risk of cascade failure. For example, backing up high-degree interdependent nodes, such as computer servers or electric transformers, to build reliability has been shown to enhance robustness of coupled systems.[64] Increasing system load capacity and evening out load—a constant challenge for large-scale electric power grids—can increase efficient management of load capacity.[65] So-called "islanding" of certain node sets to provide them alternative flow channels off of the main network—for example, providing wind or solar power through microgrids as a backup for important nodes, such as hospitals and other community services—can increase system modulatory.[66]

Similarly, systemic risk decreases when weak nodes (e.g., struggling banks) are linked to robust nodes rather than to each other.[67] Adaptive "rewiring" of a system, by changing link pathways and node connection degrees, can also deflate cascade failure through evolvability.[68] Transportation engineers, for example, are in essence in a constant effort to evolve transportation networks by adding new roads, rail lines, and so on.

Quick repair of failed nodes, particularly those closest to the boundary of remaining functional nodes, also helps prevent cascade failure.[69] After an electric grid failure, for example, repairs would start closest to the remaining functional grid components rather than at the outskirts of the failure propagation. And the selective, intentional removal of nodes and links from a system, particularly shortcut links, has been shown to reduce the continued propagation of failure even in overload failures.[70] Table 2 summarizes these strategies.

64. M.A. Di Muro et al., *Recovery of Interdependent Networks*, 6 SCI. REP., Mar. 9, 2016, at 1, https://www.nature.com/articles/srep22834 [https://perma.cc/T7KP-DZLK].

65. *Id.*

66. *Id.*

67. Sebastian M. Krause, *Controlling Systemic Risk – Network Structures that Minimize It and Node Properties to Calculate It*, ARXIV (Feb. 22, 2019), https://arxiv.org/abs/1902.08483 [https://perma.cc/XP3Z-4SRQ].

68. Tran & Namatame, *supra* note 55, at 247.

69. Di Muro et al., *supra* note 64.

70. *Id.*

Table 2. Resilience Strategies and the System Property They Enhance

Strategy	Property	Implementation
Shortcutting	Efficiency	Provide direct links between node clusters
Backing up	Redundancy	Provide replacement components for high degree nodes
Load managing	Scalability	Expand and smooth out load capacity
Islanding	Modularity	Provide alternative flow channels for identified nodes
Node pairing	Reliability	Support weak nodes through links to strong nodes
Adaptive rewiring	Evolvability	Alter and add link pathways
Severing	Reliability	Provide mechanisms to sever identified nodes from the network
Repairing	Reliability	Repair failed nodes quickly from failure boundary outward

While all of these research leads seem promising, putting them into action in real-world SETS, rather than in simulation models and purely technological systems (e.g., power grids), is an entirely different challenge.

III. CASCADE FAILURE GOVERNANCE STRATEGIES

At 1:07 p.m. on Tuesday, April 23, 2013, hackers took over the Twitter feed of the Associated Press and sent out a false tweet stating that President Barack Obama had been injured in an explosion at the White House.[71] Within seconds, retweets spread the news like wildfire. It is believed that automated stock-trading algorithms used by investment firms "read" these tweets and immediately initiated trades

71. *See* Christopher Matthews, *How Does One Fake Tweet Cause a St* [https://perma.cc/8Q6E-EUQ9]. 4, 2013), http://business.time.com/2013/04/24/how-does-one-fake-tweet-cause-a-stock-market-crash/ [https://perma.cc/8Q6E-EUQ9].

acting on the news. Then other algorithms "saw" what was going on and jumped into action as well. Over the course of a couple of minutes, the S&P 500 lost almost 1 percent of its value—about $130 billion. As the Associated Press corrected the misinformation, the market quickly rebounded, although the distribution of winners and losers likely left some traders on the short end.

Although the trading system recovered quickly from the criminal tweet, the incident illustrates how tightly wired and connected modern society has become. The social media system spread misinformation faster than humans could react with correct information; that failure jumped over to the stock-trading system, which today, thanks to automated algorithmic trading ("algo-trading"),[72] moves even faster in what are known as "subsecond networks."[73] The whole incident—a swing of $260 billion just in the S&P 500—took just a few minutes. Society is, literally, a tweet away from this kind of network cascade.

The stakes are too high—we must develop theories and practices for cascade failure governance. Research initiatives are needed to forge ground on three fronts: (1) system modeling and monitoring; (2) event prediction; and (3) event prevention, response, and recovery.

A. System Modeling and Monitoring

The first step in designing cascade failure governance is to recognize that large-scale, complex SETS permeate society and connect effects in one subsystem to others. Social inequality affects gender gaps in math;[74] job loss is linked with inequality, which is linked with poorer mental health, which is linked with lower education levels;[75] meat consumption affects human health and the environment;[76] human population trends affect food production demands, which affect biodiversity.[77] Infrastructure systems are also incredibly interconnected—the failure of a power supply unit could easily knock

72. Yesha Yadav, *How Algorithmic Trading Undermines Efficiency in Capital Markets*, 68 VAND. L. REV. 1607, 1618 (2015).

73. Neil F. Johnson, *To Slow or Not? Challenges in Subsecond Networks*, 355 SCIENCE 801, 801 (Feb. 24, 2017).

74. Thomas Breda et al., *Societal Inequalities Amplify Gender Gaps in Math*, 359 SCIENCE 1219, 1219 (Mar. 16, 2018).

75. Elizabeth O. Ananat et al., *Linking Job Loss, Inequality, Mental Health, and Education*, 356 SCIENCE 1127, 1127 (June 16, 2017).

76. H. Charles J. Godfray et al., *Meat Consumption, Health, and the Environment*, 361 SCIENCE 243, 243–45 (July 20, 2018).

77. Ellen Crist et al., *The Interaction of Human Population, Food Production, and Biodiversity Protection*, 356 SCIENCE 260, 261 (Apr. 21, 2017).

out regional oil and gas pipelines, communications systems, transportation systems, water supply and treatment systems, emergency services, banking and payment systems, and government services.[78]

Research from a wide variety of fields is converging on the need to model such vast SETS as complex adaptive systems—systems "in which large networks of components with no central control and simple rules of operation give rise to complex collective behavior, sophisticated information processing, and adaptation via learning or evolution."[79] Attributes of such systems include aspects of self-organization; network structure; emergence (the whole is different than the sum of its parts); feedback (both negative, which has a stabilizing effect, and positive, which has a destabilizing effect); the possibility of nonlinear behavior; contextualization (i.e., the application of the same approach in a different setting may not have the same results); and uncertainty.[80] From finance[81] to ecology,[82] the complex adaptive systems model is increasingly dominating how researchers conceptualize SETS dynamics.[83]

As society builds viable models of different SETS using the complex adaptive systems frame, governing cascade failure will require the capacity to install sensors and monitoring techniques to minimize time-to-failure detection.[84] For example, monitoring many properties of electric grid performance plays a large role in grid decision-making,[85] and smartphone location tracking has vastly improved real-time monitoring of traffic conditions.[86] Given what cascade failure science

78. COMM'N TO ASSESS THE THREAT TO THE U.S. FROM ELECTROMAGNETIC PULSE (EMP) ATTACK, *supra* note 11, at 12, 17.

79. MELANIE MITCHELL, COMPLEXITY: A GUIDED TOUR 13 (2009).

80. An Zeng et al., *The Science of Science: From the Perspective of Complex Systems*, 714–715 PHYSICS REP., Nov. 16, 2017, at 3–4; James Ladyman & Karoline Wiesner, *What Is a Complex System?*, 3 EUR. J. PHIL. SCI. 33, 35–38 (2013).

81. Battiston et al., *supra* note 27; Chambers et al., *supra* note 27.

82. Rika Preiser et al., *Social-Ecological Systems as Complex Adaptive Systems: Organizing Principles for Advancing Research Methods and Approaches*, 23 ECOLOGY & SOC. 46, 47 (2018).

83. Robert H. Samet, *Exploring the Future with Complexity Science: The Emerging Models*, 43 FUTURES 831, 839 (2011). For more background on the use of complexity science in a broad array of disciplines including law, see J.B. Ruhl & Daniel Martin Katz, *Measuring, Monitoring, and Managing Legal Complexity*, 101 IOWA L. REV. 191, 205 (2015).

84. Alderson & Doyle, *supra* note 45, at 841–42 (2010).

85. NAT'L AM. ELEC. RELIABILITY CORP., STATE OF RELIABILITY 2018, 41, 173 (June 2018) (discussing monitoring protocols throughout).

86. Dave Barth, *The Bright Side of Sitting in Traffic: Crowdsourcing Road Congestion Data*, GOOGLE: OFFICIAL BLOG (Aug. 25, 2009), https://googleblog.blogspot.com/2009/08/bright-side-of-sitting-in-traffic.html [https://perma.cc/NPF3-VYEA].

has revealed thus far, monitoring should focus on system features covered above as most associated with primary failure events and failure propagation: (1) areas of dense, high-degree nodes; (2) nodes with recurrent failures; and (3) shortcut links.

To be sure, building models, installing sensors, and monitoring are costly and challenging and may not be viable for all kinds of systems. Model development thus far has focused on power grids, banking, and social media.[87] Of these, social media may present more governance challenges, as platforms operate on the nebulous, global internet system. In some senses, social media platforms such as Twitter and Facebook are networks brimming with shortcut links—people connect directly with each other—as well as node-to-node pathways (e.g., through retweeting). Monitoring may be most efficient if focused on high-degree nodes with high levels of recommunication, such as so-called "influencers" and significant news outlets, such as the Associated Press. There are also large clusters of nodes in social media platforms that have self-organized into islands—more like echo chambers—within which cascading effects may be of high potential.[88]

B. Event Prediction

The point of modeling and monitoring, of course, is to predict failure events and maximize propagation detection. One technique used for power grids and banking is stress testing—putting the model under some form of discrete disturbance or load spike to see what happens.[89] Also, as real-world and simulation data are incorporated into a model, machine learning can be used to improve predictive analytics.[90] This may be particularly useful for systems prone to overload failures, given the indirect pathways of propagation.

One serious challenge for event prediction in many SETS is simply the speed of network flow. Event prediction and intervention has to work faster than event propagation. As the Associated Press tweet event demonstrates, many technological networks move at subsecond

87. Yang et al., *supra* note 3 (power grids); Huang et al., *supra* note 60; Cindy Hui et al., *Information Cascades in Social Media in Response to a Crisis: A Preliminary Model and a Case Study*, 2012 WWW '12 COMPANION: PROC. 21ST ANN. CONF. ON WORLD WIDE WEB COMPANION 653, 653.

88. Kazutoshi Sasahara et al., *On the Inevitability of Online Echo Chambers*, ARXIV (May 20, 2019), https://arxiv.org/abs/1905.03919 [https://perma.cc/XU6N-SQBS].

89. Rodrigo A. Alfaro & Mathias Drehmenn, *Macro Stress Tests and Crises: What Can We Learn?*, 4 BIS Q. REV. 29, 29 (2009).

90. Jake M. Hofman et al., *Prediction and Explanation in Social Systems*, 355 SCIENCE 486, 486 (Feb. 3, 2017); Susan Athey, *Beyond Prediction: Using Big Data for Policy Problems*, 355 SCIENCE 483, 483 (Feb. 3, 2017).

speeds. In that case, for example, to have done any good, the monitors would have to have "read" the tweet, concluded it was false, and predicted its impacts in the algo-trading network before the algo-trading network's cascade response was triggered. Given how aggressively algo-traders seek ever-faster systems,[91] this will be quite a challenge.

C. Event Prevention, Response, and Recovery

It is improbable that robust models, monitoring, and event prediction can be developed for all SETS, even if only for some of the more critical systems running society. To minimize impacts, therefore, cascade failure governance is going to have to come to grips with the need to intervene in networks in order to prevent harm and respond to and recover from harm that cannot be prevented.

In terms of network design interventions, the cascade failure science covered in Part II suggests that breaking up dense node clusters, islanding weak, vulnerable nodes, and reducing shortcut links are viable strategies. For example, banking system models suggest that prohibiting weak banks from relying heavily on other weak banks helps prevent cascade failure.[92] In social media networks, studies have shown that a small percentage of accounts are the source of a high percentage of so-called fake news.[93] Islanding them and controlling their output could help moderate failure. Capping the number of "followers" for any account and limiting the number of posts or tweets in any given time period could effectively reduce shortcut links. The rise of hyperfast networks, such as algo-trading and social media, has led some researchers to suggest that slowing down network flow could also help reduce cascading effects, although impacts of such intentional delay mechanisms in complex networks, such as stock trading, are difficult to predict.[94]

Design interventions like these would be difficult to install and, in many cases, would be highly controversial (more below in Part IV), making response and repair strategies all the more important. For responses to an event, some of the design interventions could be temporarily employed only when a failure has been detected. System delay could be imposed, shortcut links could be severed, and weak nodes could be walled off. Mechanisms for doing so would have to be in place

91. MICHAEL LEWIS, FLASH BOYS: A WALL STREET REVOLT (2014).

92. Huang et al., *supra* note 60.

93. Nir Grinberg et al., *Fake News on Twitter During the 2016 U.S. Presidential Election*, 363 SCIENCE 374, 374 (Jan. 25, 2019).

94. Johnson, *supra* note 73.

and initiated either automatically or within the time frame of human judgment. In the case of high-speed networks, the decision to implement such measures must be made very quickly.

It may not be possible to install surgical mitigation responses such as these for all kinds of networks or to implement them quickly enough and with sufficient precision. In such cases, it may be more practical to simply shut down the network temporarily, as some trading exchanges do when prices free fall[95] and as some nations have done for social media platforms in times of crisis.[96] Of course, a big question for such response measures is whether more damage is done through them than through the failure event. As the Baltimore ransomware event illustrates, shutting down a computer server network to save the servers would impose severe consequences for other systems dependent on the servers.

Postevent recovery is also a critical element of cascade failure governance. Failed nodes and links need to be repaired or replaced, and the collateral damage of the cascade failure must be addressed. As noted above, recovery strategies may be more effective by working outward from the boundary between failed and remaining system components.[97] Ironically, however, some cascade failures do not inflict any damage to nodes and links—they are a function of the network working as designed. In the Associated Press tweet event, for example, every node did what it was designed to do. In such cases, postevent recovery may need to consider redesign of the network or installation of more effective monitoring and prevention mechanisms.

IV. GOVERNANCE CHALLENGES

The previous Part engages cascade failure governance by mapping the science onto policy with the single purpose of theorizing strategies to prevent and mitigate cascade failures in important SETS. The reality of governance will present significant institutional trade-offs and normative challenges to following through on that policy approach.

---

95. *Market-Wide Circuit Breakers*, N.Y. STOCK EXCHANGE, https://www.nyse.com/markets/nyse/trading-info [https://perma.cc/4HP6-668F] (last visited Oct. 6, 2019).

96. Max Fisher, *Sri Lanka Blocks Social Media, Fearing More Violence*, N.Y. TIMES (Apr. 21, 2019), https://www.nytimes.com/2019/04/21/world/asia/sri-lanka-social-media.html [https://perma.cc/PW2R-E5ZN].

97. Di Muro et al., *supra* note 64.

A. Institutional Design

The greatest challenge to governance of cascade failure in massive SETS is their scale, which transcends multiple governance jurisdictions vertically (federal-state-local) and horizontally (organizations that cover different subject matter across federal, state, and local), and their speed, which can act in subsecond time frames. The Baltimore ransomware event was a relatively contained failure that did not propagate in any substantial sense outside of the Baltimore region. But even within Baltimore, multiple municipal departments were affected and involved in the recovery, and, as a major city, the impact surely had consequences to Maryland and the region. As Figure 1 makes clear, a cascade infrastructure failure can cross many physical and jurisdictional boundaries. Scaling this up to a multistate or national level—such as in the event of a large electromagnetic pulse (EMP) attack—presents a complete morass of intertwined and independent authorities running different pieces of the network.

Faced with this daunting institutional challenge, the commission on the EMP threat concluded in its 2017 report:

> The single most important action *that requires immediate action* to advance U.S. security and survivability is that the President establish an Executive Agent with the authority, accountability, and resources to manage U.S. national infrastructure protection and defense against the existential EMP threat (*Recommendation 1*). Current institutional authorities and responsibilities—government, industry, regulatory agencies—are fragmented, incomplete, under-resourced, and unable to protect and defend against foreign hostile EMP threats or solar superstorms.[98]

Precisely what this "Executive Agent" would look like, how it would be authorized, and what it would be authorized to do is not explained in the report. Could it direct other federal, state, and local entities, and private entities overseeing large networks, to implement network resilience strategies such as backups, islanding, and others outlined in Part II? Would it develop, or order those other entities to develop, system models, sensors, and monitoring? If it predicted a failure, would it have the authority to order severing of portions of the network? If it detects a cascade failure of international scale, can it wall off the United States? Would it have control over postfailure repair and rewiring?

On the one hand, once one appreciates the potential scale, speed, and impact magnitude of cascade failure in massive SETS, it is appealing to imagine a single entity with this kind of sweeping authority. Such an entity would be unprecedented in the federal model of governance, but the resilience strategies discussed in Part II would

98. COMM'N TO ASSESS THE THREAT TO THE U.S. FROM ELECTROMAGNETIC PULSE (EMP) ATTACK, *supra* note 32, at 1–2.

be difficult to implement without a strong, central authority to decide where to install sensors, shortcuts, and backups; which node sets to island and pair; when and how to rewire; and what system sections to sever and repair. The transaction costs and time involved to disperse these decisions throughout the system could make the decisions come too late to prevent or mitigate the failure.

Centralized or not, there are profound obstacles to implementing any kind of holistic governance regime simply as a result of how difficult it is to define the problem. Going back to Figure 1, consider some of the preliminary questions that must be answered in order to begin to design governance strategies:

- *What is the system being managed?* As Figure 1 illustrates, one could identify the banking and finance system for management, or one could take on the entire system-of-systems.

- *Who owns and manages the subsystems?* Figure 1 also illustrates the complex distribution of ownership and management, with some subsystems privately owned and managed (banking), some publicly owned and managed (government services), and some a hybrid (electric power). And even privately owned and managed systems are often subject to public regulation.

- *How are the subsystems interconnected?* Any of the subsystems in Figure 1 could be the locus of initial failure, but then what happens when it goes offline—what are the failure propagation pathways to other systems?

- *What systemic risk features are present, and where?* The governing entity or entities will need to determine where the systemic risk features (Table 1) are present in order to deploy resilience strategies (Table 2).

Once these foundations are established, the job of institutional design begins. At one level, the institutional design challenges for cascade failures seem to present familiar questions, such as degree of centralization, degree of interauthority coordination, and legal instruments for policy implementation, each of which and many more are implicated by the Executive Agent concept. But when unpacked, the cascade failure problem presents, if not a unique governance problem,

at least one that has exceptional properties that confound familiar solutions. Table 3 suggests some of these challenges.[99]

Table 3. Example Institutional Design Issues and Complications

Institutional Design Issue	Typical Design Options	Cascade Failure Complications
How should authority be distributed?	Centralized (e.g. federal preemption) versus dispersed (e.g., state primacy)	Even within a SETS of national scale, a cascade might affect only a state, a region, or the nation and can appear in different locations. Decisions made and events occurring anywhere in the SETS, even locally, can trigger cascade failure at that scale or at larger scales. Both dispersed and centralized designs may be needed.
How much and how should authorities coordinate?	Mandatory or voluntary Strong or weak	Complex interrelated infrastructure systems can involve a multitude of public and private managers, making coordination difficult.

99. For a comprehensive overview of governance design issues for problems of this scale, see ALEJANDRO E. CAMACHO & ROBERT L. GLICKSMAN, REORGANIZING GOVERNMENT: A FUNCTIONAL AND DIMENSIONAL FRAMEWORK (2019).

		Cascade failure may propagate faster than authorities can coordinate responses, in which case coordination requirements could exacerbate failure.
How strong should authority power be?	Strong or weak	Monitoring and sensor strategies require comprehensive authority over the entire SETS, and cascade failure may require swift emergency-based intervention authority, yet strong authority is expensive to support and often controversial.
What are the best instruments to use?	Prescriptive regulation, permitting, and subsidies Taxes and penalties Planning Insurance Postfailure compensation	Severing, islanding, and other strategies may require highly prescriptive measures, but rigid regulatory regimes may impede evolvability. The costs of cascade failure prevention and postfailure repair may swamp the capacity of

		subsidy, insurance, and payment programs.

B. Trade-Offs

Complex SETS provide many social benefits. As noted above, system design features that add robustness to the system's capacity to deliver such benefits can also expose the system to risk of cascade failure. But this works both ways, in that a policy single-mindedly focused on reducing systemic risk can undercut system robustness. For example, shortcut links are efficient for moving information between subsystems, and high-degree nodes are important switches in network flow. Interventions on system design that remove, suppress, or slow down such elements can impair system robustness. Anyone stranded in an airport because of a blizzard at another major airport one thousand miles away, essentially shutting down a sizable portion of the air transportation network, feels the pain that results when a network is driven by the efficiency strategy above all others. On the other hand, building redundancy (have extra jets at all airports) and modularity (switch flights around from other airports) may build resilience to failure but drive up the cost of maintaining the network. Knowing how much prevention is too much thus remains a challenge for cascade failure researchers, and the trade-off, in general, presents a difficult set of choices for policy makers as well as private entities overseeing large networks such as power networks and supply chains.

Trade-offs will also exist between subsystems. For example, adding reliability, redundancy, and modularity to infrastructure systems to build resilience could require greater physical footprints causing ecological damage. On the other hand, adding resilience to ecological resources could require that infrastructure forgo those resilience strategies, relying more on efficiency, thus threatening infrastructure resilience. Indeed, a sizable component of environmental litigation is over this tension between infrastructure resilience and ecological resilience.

C. Normative Questions

Even if a governance regime could be designed to make all the hard decisions about system management and trade-offs, it will have to navigate difficult social concerns given the intensive measures some of the resilience strategies require.

1. Defining Failure

Not all network cascades are failures. By any measure, the Baltimore ransomware event triggered a failure throughout the municipal services and payments network. The Associated Press tweet event, however, was only a failure because the tweet about the President was false. Had it been true, many market participants would have taken the rapid and precipitous drop in values to be a normal response, and the network cascade would have been congratulated. The failure was in the network's lack of capacity to detect the tweet's falsehood. Similarly, the "Arab Spring" is often held out as an example of an information cascade leveraging the internet and spilling over into political and economic networks.[100] Whether it was a cascade success or failure depends on perspective. Information cascades through trading networks and social media networks all the time. Designing systems to prevent or mitigate cascades is only half the problem—the mechanisms also need to be able to sort what society has normatively assigned to be the good cascades from the bad, do so quickly, and intervene decisively.

2. Allocating Harm

Many of the cascade failure control strategies involve imposing local harm to avoid global harm. In the case of power grids, for example, islanding areas of the network and shutting them down during event response means those areas have no power. Severing shortcut links in social media platforms would make it more difficult for some people to communicate. Repairing networks from the failed-alive boundary means components distant from the boundary suffer harm longer. Lessons learned from natural disaster preparedness and response suggest that this kind of harm allocation will present thorny issues that policy makers will need to address.[101]

3. Civil Liberties

There may be significant civil liberty constraints on how far cascade failure governance can go toward implementing prevention and response strategies. Constraining social media, for example, may raise speech regulation concerns. Shutting down parts of power grids, given the damage it can cause as critical infrastructure goes offline in severed

---

100. Charles D. Brummitt et al., *Coupled Catastrophes: Sudden Shifts Cascade and Hop Among Interdependent Systems*, J. ROYAL SOC'Y INTERFACE, Oct. 20, 2015, at 6–7, https://royalsocietypublishing.org/doi/pdf/10.1098/rsif.2015.0712 [https://perma.cc/3UV9-D759].

101. FARBER ET AL., *supra* note 25.

areas, may be claimed to be a taking of property. Fine-grained, real-time sensors and monitoring, such as through smartphone location tracking and camera surveillance arrays, likely will present privacy concerns. People depend on the networks that run SETS. Tinkering with them, even with the goal of avoiding system-wide cascade failure, will inevitably meet pushback, some of which may situate the concerns as a violation of civil liberties.

4. Social Justice

Virtually everything about SETS cascade failures triggers social justice concerns. To begin with, cascade failures generally harm those already disadvantaged disproportionately across society, such as lower income households that suffered predatory lending and foreclosures in the Great Recession and marginal fishing and other businesses that lost access to vital resources in the Gulf of Mexico in the BP oil spill. Ironically, the vulnerable node sets in those cases were not those socially vulnerable populations; they were wealthy banks and oil industry companies. Rather, the vulnerable populations took the disproportionate brunt of the cascade failure harms—they were the casualties of the failure propagation. Resilience planning must take into account these distributional concerns.

Resilience strategies must also be deployed to take into account their distributional impact, such as who bears the cost, who is protected, and the impacts of triggering strategies such as islanding and severing. For example, severing portions of an electric power grid to mitigate cascade failure will affect those who can afford backup generators and distributed power systems, such as solar panels, far less than it will those who cannot.

V. THE FATE OF ECOLOGICAL SYSTEMS

Sometime in 1986, it is believed, a commercial cargo ship left a port on the north shore of the Black Sea, destined for the Great Lakes.[102] At some point after the ship entered the Great Lakes, it discharged ballast. In that ballast were specimens of a mussel native to the North Sea aquatic system—the zebra mussel. The cascade that followed has

102. The account of the zebra mussel in this paragraph is derived from: Robert F. McMahon, *The Physiological Ecology of the Zebra Mussel,* Dreissena Polymorpha*, in North America and Europe*, 36 AM. ZOOLOGIST 339, 339, 359 (1996); Amy J. Benson et al., *Dreissena polymorpha*, U.S. GEOLOGICAL SURV. (Sept. 13, 2019), https://nas.er.usgs.gov/queries/FactSheet.aspx?SpeciesID=5 [https://perma.cc/YR4N-X9UF].

been nothing short of an ecological and economic disaster, for the zebra mussel, it seems, found its new home to be nirvana.

The life history of the zebra mussel differs greatly from most endemic Great Lakes-region bivalves, and all those differences, coupled with the different physical conditions of the Great Lakes compared to the Black Sea, gave it amazing adaptive capacities it does not enjoy in its native habitat. Zebra mussels filter water at rates far beyond endemic species, which has radically altered ecological conditions as the water is clearer and sunlight penetrates the water column deeper. Their voracious consumption of phytoplankton depletes food sources for fish. The zebra mussel attaches to almost anything, including to boats carrying them to other water bodies and to other zebra mussels, which has facilitated its propagation through most of the freshwater systems of the eastern United States. It also attaches to water intake pipes of hydroelectric and nuclear power plants, public water supply plants, and industrial facilities, creating cement-like formations that clog pipes and are costly to remove. For these and other reasons too numerous to recount here, the zebra mussel is considered the "poster child" of biological invasions.

The discussion thus far in this Article has focused primarily on the "S" and the "T" in SETS. What about the "E"—the ecological component of SETS? The zebra mussel illustrates that the "E" matters immensely to the "S" and "T."

This Article carves out the ecological component for additional treatment because this component presents both the most potentially catastrophic cascade failures and the most difficult governance challenges. It would be preposterous to attempt to do justice to the topic in one section of one article. Rather, here this Article offers a few overarching observations about cascade failures in ecological components of SETS.

First, the central point of the SETS model is that social, ecological, and technological systems are subsystems of tightly coupled, multiscalar complex adaptive systems. Social systems depend on ecological systems for their well-being through the flow of ecosystem services.[103] The resources needed to build technological systems come from ecological systems. Cascade failures in ecological systems thus threaten the robustness of social and technological systems and can trigger cascade failures there as well.[104] Yet, social and technological

103. Robert Costanza et al., *Twenty Years of Ecosystem Services: How Far Have We Come and How Far Do We Still Need to Go?*, 28 ECOSYS. SERVS. 1, 1 (2017).

104. Justin S. Brashares & Kaitlyn M. Gaynor, *Eating Ecosystems*, 356 SCIENCE 136, 136 (Apr. 14, 2017) (food gathering destroys ecosystems supplying the food, which threatens human community stability); Twila Moon, *Saying Goodbye to Glaciers*, 356 SCIENCE 580, 581 (May 12,

systems are the primary sources of cascade failure events in ecological systems.[105] In short, we and our stuff are the problem.

Second, almost none of the cascade failure governance strategies outlined in this Article will work for ecological systems directly. Aggressive islanding and severing of links have been employed with limited success in the control of some invasive species,[106] but by and large, there is very little we can do in the way of ecological network redesign and intervention to prevent and mitigate cascade failures. There is no way to rewire the oceans or wall off the Amazon. Although, one caveat here is the burgeoning research on technologies that actually would allow us to rewire and repair ecosystems, such as de-extinction methods and CRISPR gene-editing technology, both of which are actively being pursued.[107]

Third, postevent repair of ecological system cascade failures will be costly and slow. The Everglades offer a classic example of an ecological cascade failure triggered by rising phosphorous levels entering the system from agricultural and urban systems.[108] The repair effort, known as the Comprehensive Everglades Restoration Plan, has a price tag of over $10 billion and will take over thirty-five years to complete, and even then will only restore a small part of the system to its prefailure state.[109]

Finally, the two global ecological cascade failures we and our stuff have set in motion—climate change and crashing biodiversity—have already begun to trigger massive cascade failures in social and technological systems, with far more on the horizon. The ecological disruptions from climate change—altered hydrological cycles,

---

2017) (climate change from technology melts glaciers, which threatens freshwater supply to human communities).

105. Will Steffen et al., *Trajectories of the Earth System in the Anthropocene*, 115 PROC. NAT'L ACAD. SCIS. U.S. 8252, 8252 (Aug. 14, 2018); Crist et al., *supra* note 77, at 260; Aurora Torres et al., *A Looming Tragedy of the Sand Commons*, 357 SCIENCE 970 (Sept. 8, 2017).

106. Fred W. Allendorf & Laura L. Lundquist, *Introduction: Population Biology, Evolution, and Control of Invasive Species*, 17 CONSERVATION BIOLOGY 24, 28 (Feb. 2003).

107. Jonas J. Monast, *Governing Extinction in the Era of Gene Editing*, 97 N.C. L. REV. 1329, 1329 (2019); Jon Cohen, *Fields of Dreams: China Bets Big on Genome Editing of Crops*, 365 SCIENCE 422, 423 (Aug. 2, 2019); Jon Cohen, *The CRISPR Animal Kingdom: China Has Used the Genome Editor More Aggressively, on More Species, than Any Other Country*, 365 SCIENCE 426, 427 (Aug. 2, 2019). That said, de-extinction methods and CRISPR technology themselves may spawn their own cascade failures if not managed effectively.

108. Lance H. Gunderson et al., *Escaping a Rigidity Trap: Governance and Adaptive Capacity to Climate Change in the Everglades Social Ecological System*, 51 IDAHO L. REV. 127, 146, 155 (2014).

109. *Comprehensive Everglades Restoration Plan (CERP)*, NAT'L PARK SERV., https://www.nps.gov/ever/learn/nature/cerp.htm [https://perma.cc/RH5E-5QMA] (last visited Oct. 6, 2019).

species migrations, sea-level rise, ocean-temperature rise and acidification, heat waves, and many more—will trigger massive human migration, require relocation of infrastructure, alter food supply chains, and demand many more adaptation responses that will raise systemic risk to cascade failure.[110] The collapse of biodiversity will threaten the supply of ecosystem services, particularly to human populations in developing nations least able to adapt, also raising systemic risk.[111]

Managing the heightened potential for cascade failures of this magnitude and impact through the strategies outlined in this Article, even if they could be practicably implemented, would pose substantial social justice and civil liberty concerns far beyond those involved in deciding whether to shut down part of a power grid for a few days. The emerging climate justice movement[112] suggests profoundly difficult policy choices lie ahead as the threat of cascade failure spreads through SETS at all scales. In short, we are staring at a future of recurrent cascade failures in SETS of all scales throughout the world, and there may not be much we can do about them beyond adapting and repairing.

VI. CONCLUSION

Systems fail, and bigger, faster, more powerful and complex systems cause bigger, faster, more powerful and complex failures. Power grid blackouts have long attracted attention to cascade failure in technological systems; the 2008 financial collapse put a spotlight on cascade failure in economic systems; climate change threatens cascade failure in ecological systems, triggering cascade failure in human systems; cyberattacks and the sense that social media platforms are out of control are the new cascade failure policy concerns. These are not independent phenomena—they are interdependently embedded in and cascading through large-scale social-ecological-technological systems. As such, they are not independent governance propositions either; rather, they go to the essence of how policies can build resilience into SETS while balancing the systemic risk that comes with bigger, faster, more powerful and complex systems.

Governing systemic risk to cascade failure in SETS thus is as much a scientific challenge as it is a policy challenge. The science of

110. IPCC, *supra* note 17, at 9, 11.

111. INTERGOVERNMENTAL SCI.-POLICY PLATFORM ON BIODIVERSITY & ECOSYS. SERVS., *supra* note 18.

112. *See* MARY ROBINSON, CLIMATE JUSTICE: HOPE, RESILIENCE, AND THE FIGHT FOR A SUSTAINABLE FUTURE (2018); HENRY SHUE, CLIMATE JUSTICE: VULNERABILITY AND PROTECTION (2014).

cascade failures in social, ecological, and technological systems seeks to understand their causes and behavior and is developing metrics and principles for describing systemic risk, failure propagation, and network resilience. Governance institutions can benefit from the techniques and strategies cascade failure science is exploring for modeling, monitoring, event prediction, and event prevention, response, and recovery. Yet these techniques and strategies could present difficult policy choices. How much censoring can governance institutions impose on people and businesses? Should we sacrifice some of the power of social media or the banking system to reduce cascade failure risk? Who decides what is or is not failure, and who decides which populations are islanded from power or communications?

Legal scholars and practitioners have an important role to play in resolving these questions. But rather than developing legal responses for power grids, banking, social media, and other systems one by one, a general legal theory of cascade failures is as critical to formulate as is a general scientific theory. What are the *legal* techniques for deploying system sensors, severing shortcut links, slowing down system speed, islanding system parts, and building system modularity? What *legal* concerns arise from using any of these techniques? With climate change underway, cascade failures in SETS will only become more common and more serious. This Article hopes to demonstrate that a legal theory of cascade failure is desperately needed if they are to be effectively governed.