A COMPLEX ADAPTIVE SYSTEMS THEORY OF HOMELAND SECURITY

LEWIS, TED, G., Center for Homeland Defense and Security,
Naval Postgraduate School (Ret.)
tedglewis@icloud.com

ABSTRACT

Homeland security is an eclectic field of study that seeks to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risks to the U.S. This article applies the theory of complex adaptive systems (CAS) to homeland security, finding that CAS offers strategies to mitigate the risks and fragility of homeland security policy and practice.

INTRODUCTION

Comiskey (2018) states that homeland security lacks a grand theory or overarching framework. Essentially, homeland security is an eclectic field of study that seeks to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risks to the U.S. The body of knowledge considered homeland security has evolved rapidly over the past 20–50 years. Roughly speaking, it is a hybrid of leadership, risk management, security, social identity, and terrorism themes centered around nine knowledge domains: critical infrastructure and resilience, emergency management, human and environmental security, intelligence, law and policy, professionalism, risk management, strategic planning, and terrorism.

This paper provides a theory of homeland security based on complex adaptive systems (CAS), defined as systems in which many independent elements or agents interact, leading to emergent outcomes that are often difficult or impossible to predict simply by looking at individual interactions (Project Guts, n.d.). This approach seems appropriate because of the homeland security enterprise's many independent elements and agents and the problematic or impossible-to-predict incidents that make homeland security a challenging discipline. In addition, homeland security is emergent because new threats and challenges always appear, requiring adaptation. It is truly multidisciplinary and interdisciplinary.

COMPLEX ADAPTIVE SYSTEMS AND HOMELAND SECURITY

CAS is a good match with homeland security. Both are concerned with unexpected, disruptive incidents. Both deal with many moving parts simultaneously and exhibit the emergence of threats and responses from individual interactions. Moreover, both evolve continuously as causal factors shape and direct them. Deputy Secretary of Defense Ashton Carter (2013) defined *complex catastrophes* as natural or man-made incidents, including cyberspace attacks, power

grid failures, and terrorism, resulting in cascading failures of multiple, interdependent, critical, life-sustaining infrastructure sectors and causing extraordinary levels of mass casualties, damage, or disruption severely affecting the population, environment, economy, public health, national morale, response efforts, and government functions. Carter identified causal factors in homeland security and suggested the goal of a homeland security enterprise—to protect the population, environment, economy, public health, national morale, response efforts, and government functions.

The author extends Carter's (2013) definition to the broader organizational issues surrounding the homeland security enterprise. This theory encompasses complex catastrophes of both organizational failure and physical/cyber failure. This author identified six causal factors of CAS drivers in a complex environment: the tragedy of the commons, the paradox of enrichment, the paradox of redundancy, competitive exclusion, exponential contagion, and co-evolution. There are costly consequences to incidents in the CAS, which we must study and understand to mitigate or eliminate. The CAS theory must be actionable to prevent, deter, and respond to natural and human-caused adverse incidents that may occur due to organizational failure, natural incidents, or perpetrated attacks. Therefore, an actionable theory must be implementable in the real world—it must be capable of deterring, preventing, and responding to disastrous and catastrophic events. CAS includes sensing and responding: sensing involves measuring risk and resilience; responding involves prevention, deterrence, response, and adaptation.

CAS theory was developed over the years since 9/11, inspired by the work of Perrow (1999), Bak et al. (1987), Bak (1996), Lewis (2011), and Kaufmann (1993). Perrow (1999) was perhaps the first person to study catastrophic events in terms of chain reactions, beginning with small errors that cascade and grow in size as they propagate through a system. He attributed catastrophic collapse to management failure. Bak et al. (1987) refined the idea of small faults percolating through a system, ending in disaster. They used a land-sliding sand pile as a metaphor for complex systems and showed that complex systems obey a power law of frequency versus the size of the incident instead of a normal distribution. As it runs out, power law distributions of frequency versus consequence indicate the inner workings of a complex catastrophe. Kauffman (1993) described how life emerged from non-living things through self-organization. The idea of self-organization and emergent behavior completes the CAS theory.

Lewis (2020, 2022) extended the work of Perrow (1999), Bak et al. (1987), Bak (1996), and Kaufmann (1993) to understand and explain collapses in critical infrastructures. He extended the theory of collapse of critical infrastructure to homeland security by combining the theories of self-organization, emergent behavior, efficiency, and optimization—all leading to failures of organizations and processes. Lewis identified complex adaptive behaviors called *causal organizing principles* responsible for the emergence, over time, of fragility in physical, cyber, and organizational structures, leading to heightened risk and fragility. Roughly speaking, risk and fragility emerge because systems seek order, efficiency, and optimal operation. Bak's (1996) *punctuated equilibrium* states that order, efficiency, and optimization increase until reaching a critical point whereby the system collapses, and the process repeats. Furthermore, the frequency

of collapse obeys a power law with an exponent indicating the degree of severity of the threat. Thus, the degree of catastrophe can be quantified and used to measure risk and fragility.

Bak's (1996) observation that systems collapse because of efficiency and optimization may seem heretical in today's hi-tech world. However, there are many examples to prove his point. The result of optimization applied to the U.S. supply chain, which lacked surge capacity and redundancy, illustrated clearly the danger of optimization in 2022. By optimizing the supply chain to be "mean and lean," operators eliminated its resiliency and tolerance for demand surges, redundant ports, and elastic demand. Modern society is replete with examples of optimized systems that eventually collapsed (Lewis, 2020, 2022).

THE MODEL

Only by understanding CAS's causal factors can we devise means of reducing risk and increasing the resilience of physical, cyber, and organizational systems. In the next section, the author identifies six causal factors observed in practice and suggests strategies for mitigating the resulting risk and fragility. This is not a complete list—one can imagine other causal factors that shape the threat surface through self-organization.

Following the lead of Hodges (2015, 2016, 2019), the author defines homeland security in terms of CAS's causal factors, as shown in Figure 1. Hodges identifies sustainability, stability, and adaptability as causal factors and relates them to the mission of homeland security enterprise. In our model, the homeland security enterprise continuously scans the horizon to sense gathering and impending trouble. Sensing involves measuring and interpreting data—a typical intelligence operation. The results are summarized in terms of risk and resilience. The resulting risk and resilience summaries are used to adapt, plan, and allocate resources that reduce risk and enhance resilience.

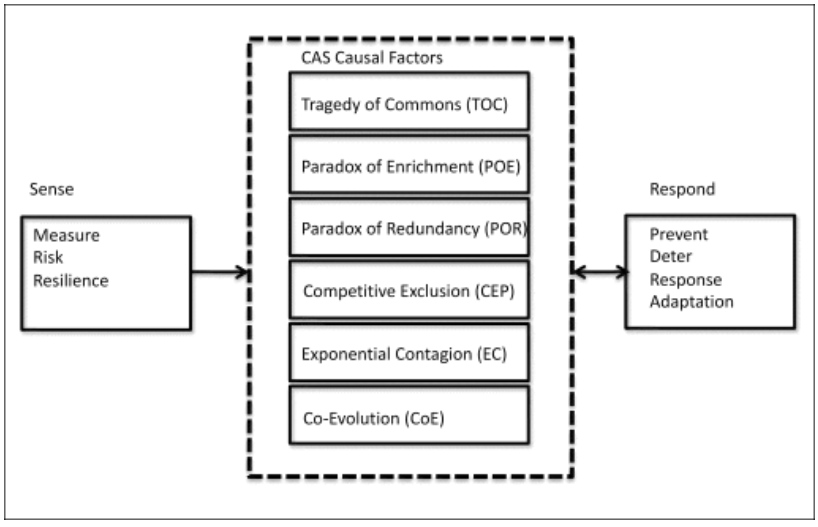

Figure 1. CAS theory model: Continuously sense, respond, and adapt to unexpected incidents.

Risk is *expected loss* due to threat, and resilience is a two-dimensional function of consequence and time. That is, resilience decreases as the consequence and time to respond to an incident increase. Mathematically, risk is defined in terms of frequency of incidents of consequence x_i, and resilience Z in terms of risk R and time-to-recover, Δt, as follows (Lewis, 2022):

$$f(x_i): frequency\ of\ incident\ of\ size\ x_i; i = 1, 2, 3, \ldots n$$

$$EP(x_i) = \sum_{j=i}^{j=n} f(x_j) : exceedance$$

$$R(x_i) = x_i * EP(x_i)$$

$$Z = h(R, \Delta t)$$

These assessments may be qualitative or quantitative. For example, Figure 2 illustrates a quantitative assessment of the risk of cyberattacks on information systems. Actual data is converted into a plot of exceedance (the frequency of attacks that equal or exceed a consequence) and fitted to a long-tailed power law. Risk is simply the product of consequence (x-axis) and exceedance (y-axis). The calculation of resilience is not shown.

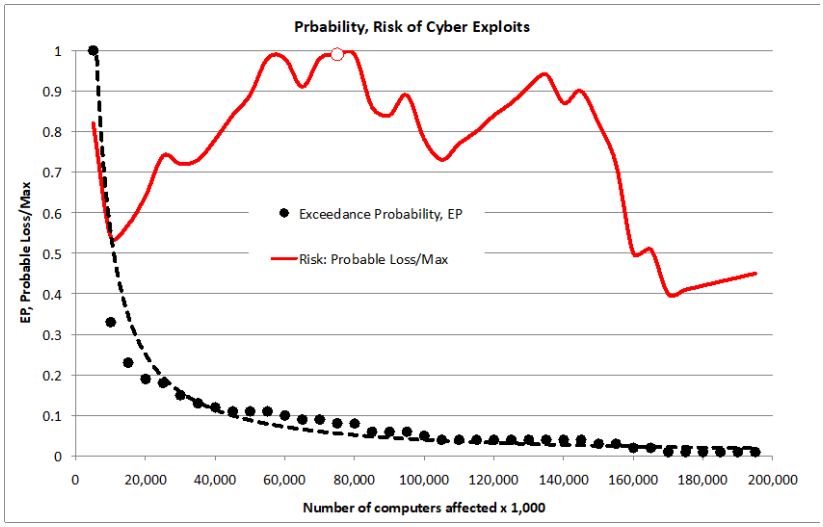

Figure 2. Quantitative risk assessment of cyber-attacks on information systems. Dots are the exceedance frequency obtained from actual data of reported attacks; the dotted line is a power law fit to the data; and the solid red line is risk. Risk here is particularly long-tailed, suggesting the likelihood of a Black Swan incident.

Qualitatively, risk and resilience may be reported as high, medium, or low, according to expert opinion. Hodges suggests a qualitative point system for estimating risk and resilience, whereas Lewis (2020, 2022) gives mathematical formulas for calculating risk and resilience. A variety of risk and resilience measures have been proposed in the literature. They are beyond the scope of this paper. At the opposite end of Figure 1 is the response box. Given conditions that are sensed, a homeland security enterprise must continually adjust and adapt to what is sensed. This is done

by tracking the dynamics of self-organizing "threats" and "hazards." A proactive organization understands the principles of operation of emerging threats and hazards and prepares to deal with them. Reacting to various threats and hazards is the task before every homeland security enterprise and the central theme of the proposed CAS theory.

CAUSAL FACTORS

Causal factors are a byproduct of self-organization. Essentially, self-organization is a process of replacing disorder with order, optimization, and adaptation. As organizational, physical, and cyber systems age, they become brittle and susceptible to failure due to human action, nature, or wear and tear. Bak's (1996) punctuated equilibrium theory is recurrent—self-organization builds over time, reaches a critical point, fails, and repeats. Self-organization manifests in different ways, which are captured as causal factors.

The most common form of self-organization is *preferential attachment* (PA). PA emerges from randomness into order or structure of some sort. Typically, the structure emerges as a hub or centralization of assets or command and control. The hub-and-spoke structure of commercial airliner routes is an example. Reliance on a single command post, the concentration of assets onto a single law enforcement computer, and the production of vaccines at a single global plant are three other examples. All of these increase the risk of failure due to a single point of failure. They are almost always the result of optimization for efficiency.

There are other, more subtle forms of self-organization, as listed here with examples. In each case, destabilization increases vulnerabilities that terrorists can exploit, or the risk of damage caused by natural hazards. Self-organization almost always produces an efficient organization or structure with single points of failure or subtle vulnerabilities. They are the root cause of failure but are often disguised as something more subtle.

Tragedy of the Commons

The *tragedy of the commons* (TOC) occurs when greedy stakeholders optimize their self-interest at the expense of other stakeholders ("Tragedy of the Commons," 2023). Systems typically have a finite carrying capacity—a resource of some sort. For example, the adoption of electric vehicles (EV) may lead to exceeding the carrying capacity of the roads in the U.S. because EV owners do not support the maintenance of roads through payment of a gasoline tax. U.S. roads are not sustainable without gasoline taxes. Other examples of TOC are over-fishing the ocean, all-you-can-eat internet bandwidth use, unlimited power grid use by producers and consumers, and free and unlimited access to medical care. In general, unlimited use of a commons without feedback to limit its use will lead to an open system TOC.

Paradox of Enrichment

Is it possible to have too much of a good thing? The *paradox of enrichment* (POE) says that whenever a system attempts to absorb too much capacity, money, resources, etc., it begins unbalancing due to an excess. For example, the *Braess paradox* says that adding a road to a road network, hoping to improve traffic flow, can slow down traffic ("Braess Paradox," 2023). Another example is the 2008 financial collapse. Leading up to 2008, subprime loans made financing a home extremely easy. However, this enrichment led to ruin when the carrying capacity of home ownership was exceeded. The carrying capacity of home ownership in the U.S. is approximately equal to the fraction of the working population—64%. The financial collapse resulted when this capacity was exceeded ("Paradox of Enrichment," 2023).

Wall Street bankers are familiar with POEs such as *Minsky moments* and *Dutch diseases*. A Minsky moment occurs whenever the price of stocks exceeds their carrying capacity, and buyers vanish (Ganti, 2022). The stock market collapses due to too much money being followed by too few buyers. This is another example of enrichment leading to collapse instead of improvement—a counter-intuitive idea. The Dutch disease illustrates enrichment's slightly different effect on a financial system ("Dutch Disease," 2023). It is called a Dutch disease because it happened in the Netherlands in 1959 when the energy sector was enriched (by the discovery of natural gas offshore) at the expense of the other sectors. Enrichment meant the price of food and rent skyrocketed, leaving non-energy workers unable to keep up. Other sectors suffered because one sector was enriched. Destabilization from enrichment is just as detrimental as poverty from inadequate resources.

Paradox of Redundancy

Security experts generally consider redundancy beneficial, and in most cases, it is. However, when it comes to information systems, redundancy may become a weakness. This is referred to as the *paradox of redundancy*. For example, running two or more computers—a primary one and a redundant spare—can become a liability if the redundancy increases the threat surface. More computers mean more cost and more opportunity for hackers to attack the information system. Specifically, backup computers on standby may become infected with malware, becoming an added vulnerability.

Another, more subtle form of redundancy leads to greater risk and less resilience—the *standard.* Industry establishes standards for interchangeable parts, ease of maintenance, and lower production costs. However, standards can also be attacked. For example, the transmission control protocol/internet protocol (TCP/IP) standard required by all computers connected to the internet makes the internet work globally. However, it also makes it easy to attack everywhere. An attack on one TCP/IP connection is an attack on all TCP/IP connections, which is every internet connection in the world. The internet is loaded with standards—all vulnerable to a standard malware attack. Oddly, older pre-internet standards are more secure than modern internet-standard connections and protocols. This is related to the *competitive exclusion principle*.

Competitive Exclusion Principle

The competitive exclusion principle (CEP) was first articulated by Gregory Gause, a Soviet biologist, and elaborated by Joseph Grinnell, an American naturalist interested in competition among species (Britannica, 2023; "Competitive Exclusion Principle," 2023). It states that in an ecological niche where species compete, only one will dominate over all others because a small advantage on the part of one species is marshaled into a major advantage, resulting in dominance or monopoly.

CEP often results in a monoculture, as illustrated by TCP/IP and internet standards. Monocultures are notoriously easy to attack because a successful exploit works everywhere. Monocultures and monopolies, as we already know, reduce redundancy and surge capacity. It is why most regions of the U.S. have only one hospital, fire department, and police department. CEP leads to single cable and internet service providers and diminishing production facilities for drugs and vaccines. It is an example of optimizing for efficiency, according to Bak. It also introduces single points of failure. The energy, power, law enforcement, and emergency services sectors suffer the most from CEP. Tax and ratepayers do not want to pay for redundancy; hence, economics is a main driving force. Redundancy and surge capacity come at a price. Monocultures can only be reversed by adding costly diversity and non-standard parts to a system. However, if the cost of recovery is high, the cost of prevention may be worthwhile.

Exponential Contagion

The COVID-19 pandemic is a dramatic example of the power of exponential contagion, but this self-organizing principle is also a powerful force for propelling misinformation and lies online. Social networks and COVID-19 work similarly—they spread contagion at lightning speed because they are exponential technologies. The rapid speed and impact of exponential contagions are especially problematic for homeland security because of the requirement for quick response. In a matter of days or hours, a biological contagion or internet misinformation/malware can spread worldwide. Without an early warning system, this kind of threat can be as dangerous as a physical attack.

Unfortunately, due to the distributed nature of its origin, exponential contagion is difficult to deter, prevent, and respond to. This was demonstrated by delayed responses to COVID-19 and nearly impossible countermeasures aimed at misinformation related to the 2020 U.S. presidential election. Moreover, because they are asymmetric, exponential contagions will grow in frequency and consequences. Figure 2 shows that malware is an especially long-tailed threat and ripe for black swans. Contagions blow up into massive cascades with corresponding consequences. They can manifest as internet malware, misinformation, disease, and political actions (Ifioque, 2023).

Co-Evolution

Co-evolution (CoE) occurs when two (or more) species reciprocally affect each other's evolution. That is, the development of one species depends on the development of others, and conversely, the development of the others depends on the one species. Business co-evolution is similar—the evolution of computers depended on the internet, and conversely, the internet's evolution depended on computers. The two are dynamic and interdependent (Hodges, 2019).

Regarding terrorism, it is very important to consider co-evolution as a form of enhancing the capabilities of terrorists. The Transportation Security Administration's (TSA) experience with attempts on commercial airliners is an example. Following 9/11, the TSA began inspecting passengers using scanners at airports. The terrorists responded by concealing weapons in their shoes. When the TSA improved inspection by requiring passengers to remove their shoes, the terrorists developed liquid explosives. The TSA responded once again, each iteration strengthening the terrorist capability. The evolution of terrorism and TSA security illustrates co-evolution. The homeland security enterprise must co-evolve like a biological species because terrorists constantly improve. The drug cartels are learning organizations that learn and adapt to deviant innovation (Santana, 2023). As border security tightened, cartels used submarines to move drugs. When the U.S. Coast Guard defended against submarines, the cartels adopted drones. The homeland security enterprise must recognize co-evolution as a causal factor and adapt faster than the opposition.

THEORY TO PRACTICE

The foregoing analysis of CAS applied to homeland security suggests a few strategies for dealing with the vulnerabilities identified above. The following list assumes that the stated homeland security goals are recognized across the enterprise. However, note that opinions differ on what the goals are. The author lists three possible applications of CAS theory to practice.

Threat Outpaces Available Resources

First and foremost is recognizing that cost and time resources are limited while the threat is not. This asymmetric attack surface is the most challenging of all—homeland security will always be under-resourced compared with the challenge. Hence, risk/resilience sensing aims to apply limited resources to the highest need. Instead of resourcing every asset and organization equally, the smart strategy is to apply resources where they do the greatest good. Assuming one can sense tail risk, as shown in Figure 3, the following rule should be applied.

> *Strategy: Limited resources should be used to* prevent *black swans, while they should be used to* respond *to lesser incidents—gray swans.*

Examples of gray swans are fires in cities, traffic accidents, mild hurricanes, crime, and domestic terrorism. For example, local firefighters and law enforcement/EMS respond to fires in cities and

traffic accidents. Examples of black swans are forest fires, war, pandemics, and mega-floods. Good forest management practices, negotiations among nations, global sensing of contagions, and climate change policies prevent forest fires, wars, pandemics, and mega-floods.

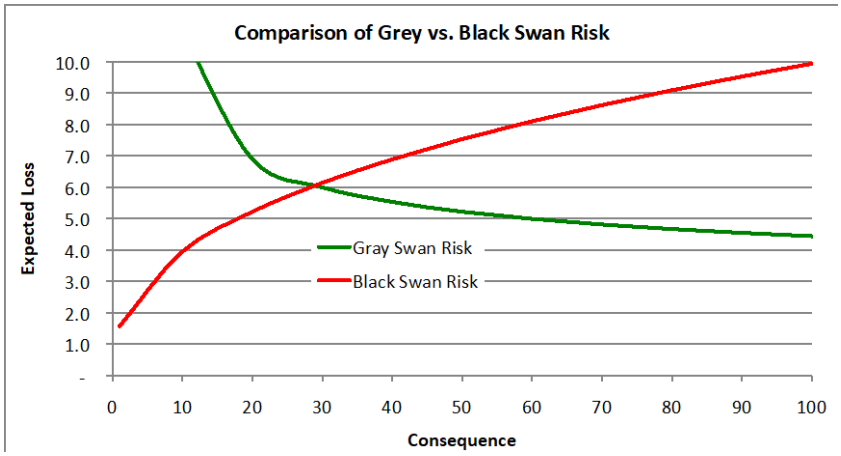

Figure 3. Gray swan incident risk declines with consequence, while black swan risk increases. This suggests that it is best to resource prevention of black swans and resource response to gray swans.

Resilience Versus Efficiency

One of the primary goals of the homeland security enterprise is to enhance resilience by partnering with industry and governments. Industry needs to strengthen infrastructure systems they own and operate, and the government must enact regulations promoting resilience. Theoretically, the loss of efficiency and non-optimality is offset by the advantages of resilient organizations and infrastructure—the ability to accommodate surges and adapt to unexpected faults. However, this has to be proven by favorable results.

Forest fires in California in 2018 cost the U.S. economy $148 billion (Wang et al., 2021). Most could have been prevented by placing power transmission lines underground for far less. Between 2019 and 2021, 56 hurricanes caused $2.7 trillion in damage to infrastructure and homes (Smith, 2022). Much of this could have been prevented by burying utility lines underground, addressing climate change, and removing homes from near the ocean. While costly, prevention appears less expensive than response after the fact.

The homeland security enterprise must work with industry and government to examine the true costs of efficiency. By ignoring costly externalities such as extreme weather caused by carbon emissions, the reduction in supply chain costs by eliminating redundancy, or the trade-off between above-ground power lines versus expensive underground lines, the homeland security enterprise misses an opportunity to secure the homeland.

Strategy: Cost-benefit analysis of resilience versus efficiency should include the true costs of "efficiency" versus the costs of redundancy, surge capacity, hardening, and other "non-optimal" measures.

Apply Network Effects to Homeland Security

Increasing returns and network effects remind us of *Metcalf's law*, which says the power of a network increases with the square of the number of nodes ("Metcalf's Law," 2023). This is another way of expressing synergy within a CAS system that comes from complexity. That is, capability exponentially increases simply through connectivity. The capabilities of the whole are greater than the sum of the capabilities of individuals. Increasing returns has been described as the rich get richer—the same self-organizing property of Gause's competitive exclusion principle. When applied to strategy, a good strategy leverages network effects to magnify resilience and ability to tolerate stress. Shared responsibility is a strategy of spreading risk across many parties and/or layers of a system. One of the best illustrations of this is how the U.S. Forest Services within the Department of the Interior spread responsibility for fighting forest fires across local, tribal, state, and federal jurisdictions. When a major forest fire breaks out in California or Washington, every firefighting unit in the 11 Western States responds.

The Price-Anderson Act that re-insures nuclear power plant owners against catastrophic failure of any of the 90+ nuclear power plants in the U.S. spreads risk across all owners and operators and the Federal government. All 90+ nuclear power plant owners share in the cost of any one power plant disaster when the cost exceeds a certain amount. Thus, owners and operators are incentivized to prevent accidents. Shared responsibility means everyone in the network is responsible for everyone else. The weakest link becomes a liability for all. For example, cybersecurity is a global community issue. Instead of leaving each server to its defense, suppose internet security is a community responsibility. The network effect of the highly connected internet suddenly becomes an advantage instead of a liability. The same idea applies to other sectors, such as public health and fighting terrorism.

Strategy: Leverage network effects within the homeland security enterprise to magnify prevention and response.

CONCLUSION

Homeland security is a wicked problem. The complex adaptive systems theory offers effective strategies to manage homeland security's myriad threats and hazards. The homeland security enterprise should focus on gray swan events and dedicate limited resources to black swan events. Their cost-benefit analyses should consider true efficiency costs, redundancy benefits, and the leveraging of networks.

REFERENCES

Bak, P. (1996). *How nature works: The science of self-organized criticality*. Copernicus Press.

Bak, P., Tang, C. & Weisenfeld, K. (1987). Self-organized criticality: An explanation of 1/f noise. *Physical Review Letters*, *59*, 381–384.

Braess paradox. (2023). In *Wikipedia.* https:/en.wikipedia.org/wiki/Braess%27s_paradox

Britannica. (2023). The principle of competitive exclusion. In *Britannica.* https://www.britannica.com/science/principle-of-competitive-exclusion

Carter, A. B. (2013, February 19). *Definition of the term complex catastrophe*. Department of Defense. https://dde.carlisle.army.mil/documents/courses_13/Readings/2338_Catastrophe.pdf

Comiskey, J. (2018). Theory for homeland security. *Journal of Homeland Security Education*, *7,* 29–45, https://jsire.org/theory-for-homeland-security

Competitive exclusion principle. (2023). In *Wikipedia*. https://en.wikipedia.org/wiki/Competitive_exclusion_principle

Dutch disease. (2023). In *Wikipedia*. https://en.wikipedia.org/wiki/Dutch_disease

Ganti, A. (2022). *What is a Minsky moment? Definition, causes, history, and examples*. Investopedia. https://www.investopedia.com/terms/m/minskymoment.asp

Hodges, L. (2015). *Systems fragility: The sociology of chaos.* [Master's thesis, Center for Homeland Defense and Security, Naval Postgraduate School]. https://www.hsaj.org/articles/4768

Hodges, L. (2016). Systems fragility: The sociology of chaos. *Journal of Emergency Management*, *14*(3), 77–87. doi: 10.5055/jem.2016.0284.

Hodges, L. (2019). The quantum physics of emergency management. *Journal of Business Continuity and Emergency Planning*, *12*(2), 150–157

Ifioque. (2023). *Contagion theory*. https://ifioque.com/social-psychology/contagion-theory

Kauffman, S. A. (1993). *The origins of order: Self-organization and selection in evolution*. Oxford University Press.

Lewis, T. G. (2011). *Bak's sand pile: Strategies for a catastrophic world*. Agile Press.

Lewis, T. G. (2020). *Critical infrastructure protection in homeland security: Defending a networked nation*. (3rd ed.) John Wiley & Sons.

Lewis, T. G. (2022). The mathematics of catastrophe. *AppliedMath*, *2*, 480–500.

Metcalf's law. (2023). In *Wikipedia.* https://en.wikipedia.org/wiki/Metcalfe's_law

Paradox of enrichment.(2023). in *Wikipedia.* https://en.wikipedia.org/wiki/Paradox_of_enrichment

Perrow, C. (1999). *Normal accident theory*. Princeton University Press.

Project Guts. (n.d.). *What is a complex adaptive system?* Code.org. https://code.org/curriculum/science/files/CS_in_Science_Background_papers.pdf

Santana. J. J. (2023). *Deviant innovation*. jsantana.org. https://www.jsantana.org/deviant-innovation

Smith, A. B. (2022, January 24). *2021 U.S. billion-dollar weather and climate disasters in historical context.* Beyond the Data. https://www.climate.gov/news-features/blogs/beyond-data/2021-us-billion-dollar-weather-and-climate-disasters-historical

Tragedy of the commons (2023). In *Wikipedia*. https://en.wikipedia.org/wiki/Tragedy_of_the_commons

Wang, D., Guan, D., Zhu, S., MacKinnon, M.M., Geng, G., Zhang, Q., … Davis, S. J. (2021). Economic footprint of California wildfires in 2018. *Nature Sustainability*. 4, 252–260, https://doi.org/10.1038/s41893-020-00646-7