

The Red Pill of Resilience

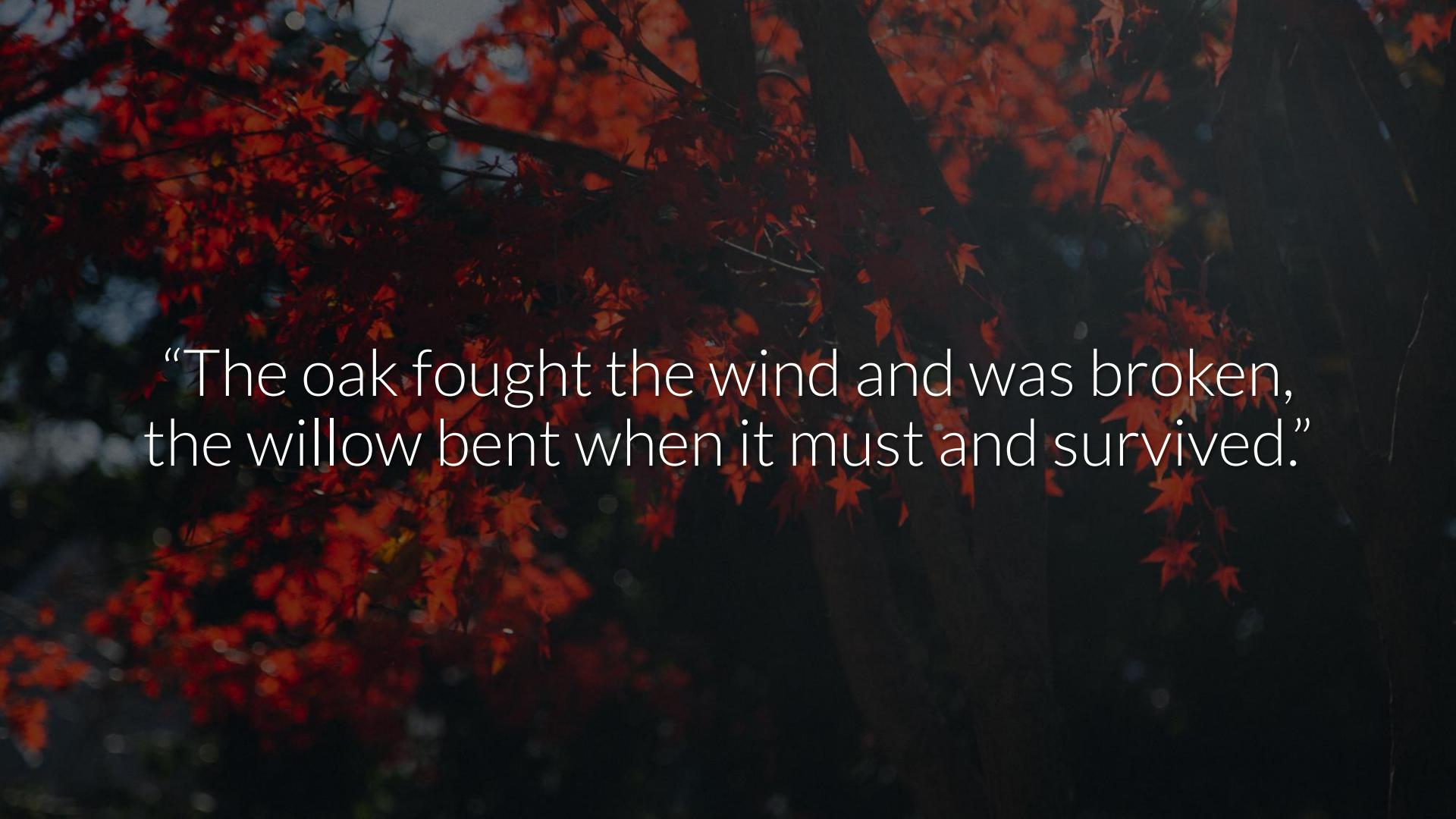
A close-up photograph of two hands clasped together, illuminated by red and blue light against a dark background. The hands are positioned in the center of the frame, with fingers interlocked. The lighting creates a dramatic effect, with one hand appearing mostly red and the other mostly blue.

Kelly Shortridge (@swagitda_)
Rochester Security Summit 2017

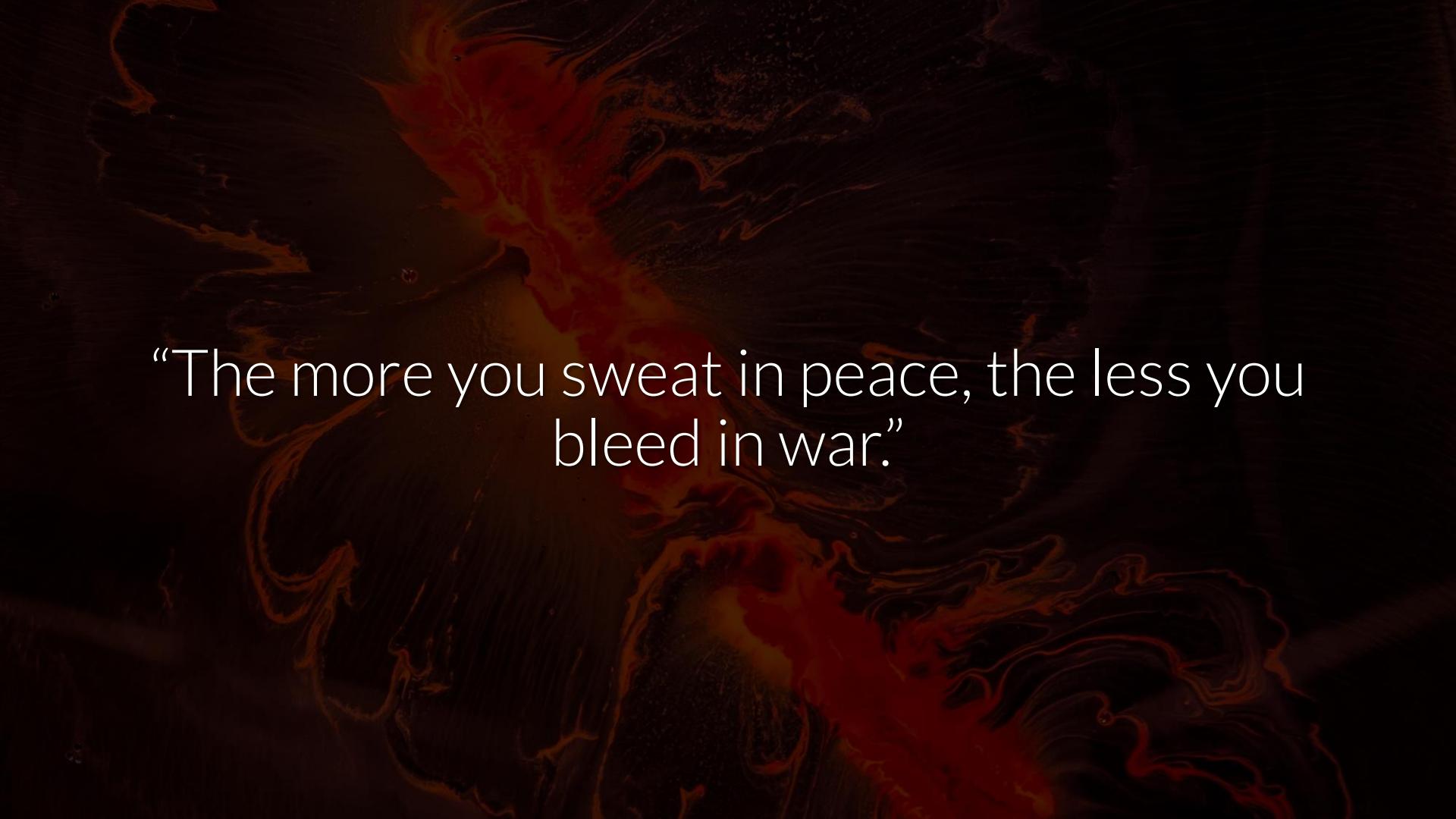
A gray tabby cat stands in a thick layer of fallen autumn leaves. The leaves are a mix of red, orange, yellow, and brown. The cat is positioned in the center of the frame, facing away from the camera. Its tail is raised and curved over its back. The background is a wire mesh fence.

Hi, I'm Kelly

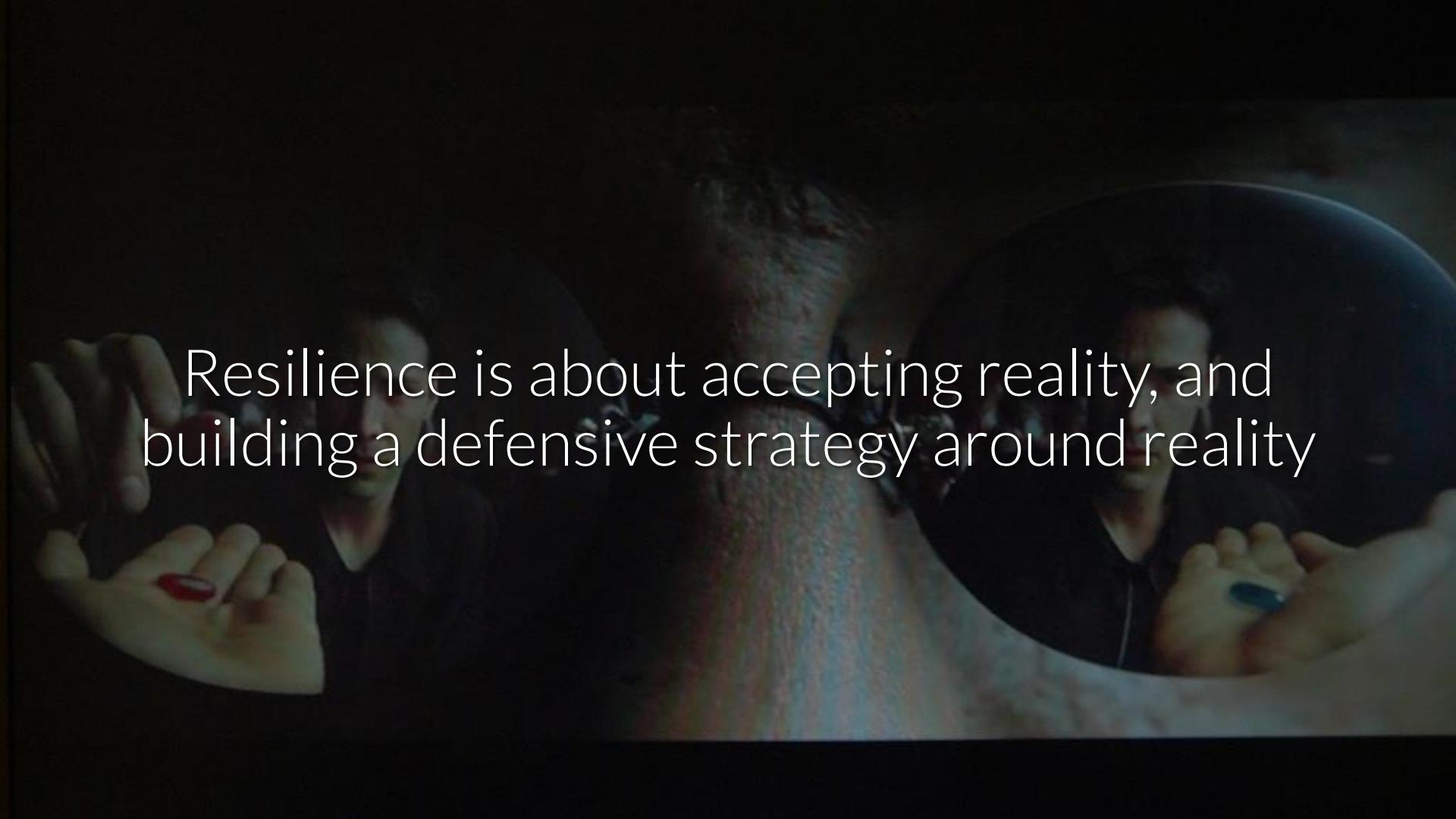
Resilience begets deterrence

A dark, moody background featuring a cluster of vibrant red autumn leaves in the center. The leaves are sharp and detailed against a dark, slightly blurred background.

“The oak fought the wind and was broken,
the willow bent when it must and survived.”



“The more you sweat in peace, the less you bleed in war.”

A dark, moody photograph showing two people in a close embrace. One person's face is partially hidden behind the other's hair. The lighting is low, creating a somber and intimate atmosphere.

Resilience is about accepting reality, and
building a defensive strategy around reality

Stages of Grief in InfoSec

Etymology of Resilience

The Resilience Triad:

- Robustness
- Adaptability
- Transformability



Stages of Grief

InfoSec is grieving that companies will never
be invulnerable to attack

Denial – clinging to a false reality

“We aren’t really at risk”

Anger – frustration that denial can't go on

“It's your fault that I need security”

Bargaining – hope that the cause is avoidable

“Maybe we can stop attacks from happening”

Depression – despair over the reality

“We’re going to be hacked, why bother?”

Acceptance – embracing inevitability

“Attacks will happen, but I can be prepared”



Lack of acceptance feeds solution
fragmentation, FUD, and snake oil

Security nihilism isn't the answer.

Resilience is.

Etymology of Resilience

1858: Engineering - strength & ductility

20th Century: Psychology, ecology, social sciences, climate change, disaster recovery

Resilience in Complex Systems

Non-linear activity in the aggregate

Intertwined components, unpredictability

Infosec is a complex system.

Defenders, attackers, users, governments,
software vendors, service providers, ...

The background image is a dramatic, low-light photograph of a mountainous landscape. In the center, a sharp, snow-covered peak rises against a dark, cloudy sky. The foreground is filled with the silhouettes and warm-toned foliage of trees, likely aspens, showing autumn colors. The overall mood is somber and powerful.

Ecological resilience

Continually adapt; high degree of instability



Chestnut trees in eastern North America's forests were wiped out by chestnut blight

Oak and hickory trees grew in their stead

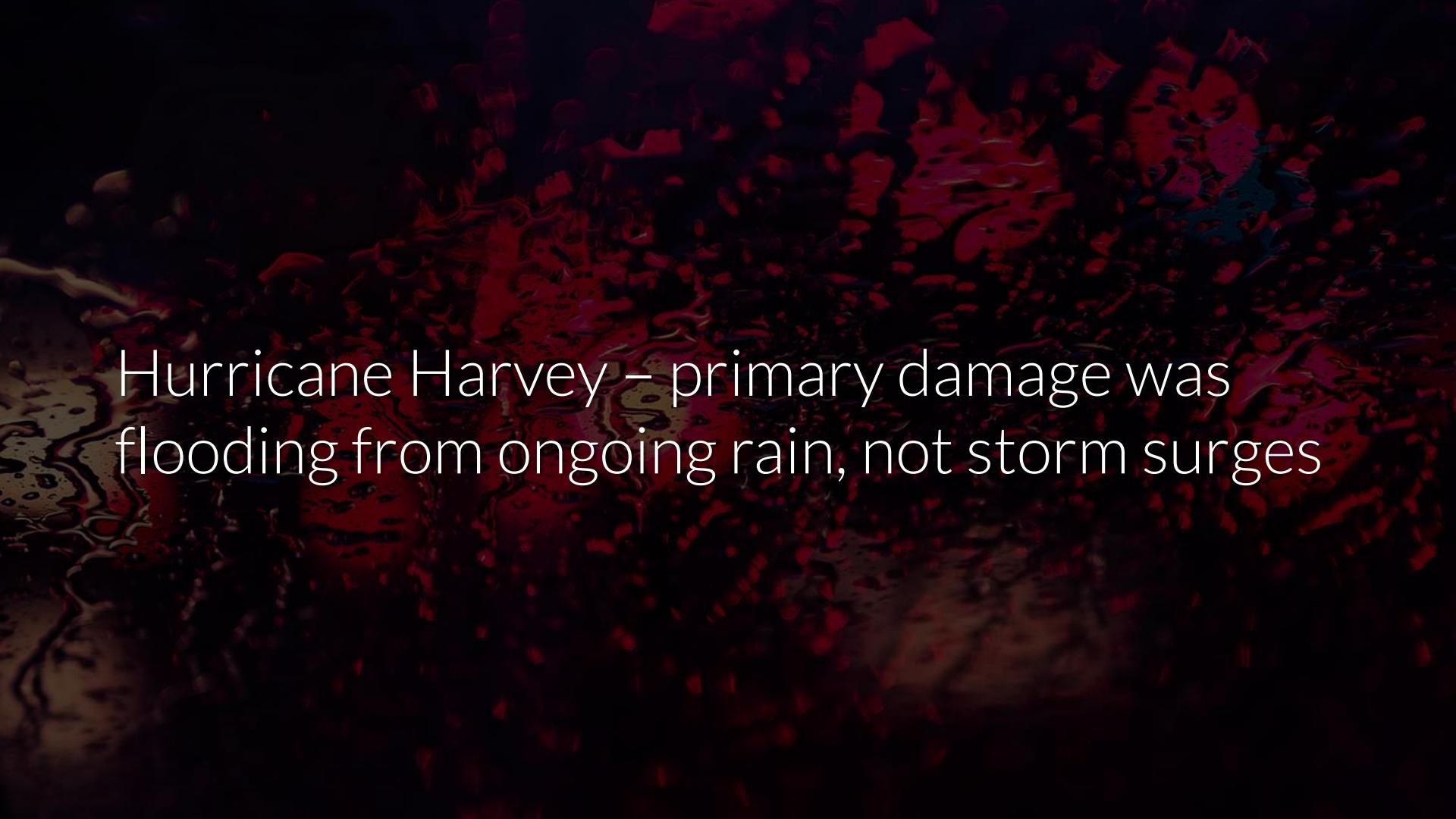
Evolutionary resilience assumes socio-ecological systems are co-evolutionary



Communities can diversify agricultural landscapes and production systems

Three central characteristics of resilience:

Robustness, Adaptability, Transformability



Hurricane Harvey – primary damage was flooding from ongoing rain, not storm surges

A photograph of a traditional Japanese garden path. The path is paved with dark stones and leads through a series of red torii gates, which are traditional Japanese gate structures. The gates are arranged in a perspective that leads the eye towards a small, traditional-style lantern hanging from one of the gates. The scene is set at dusk or night, with the path illuminated by the lantern and the surrounding area in deep shadow.

Resilience is about the journey, not the destination

Accept the risk will exist

Reduce potential damage & restructure
around the risk

Survival rests on embracing the unknown
and accepting that change is inevitable

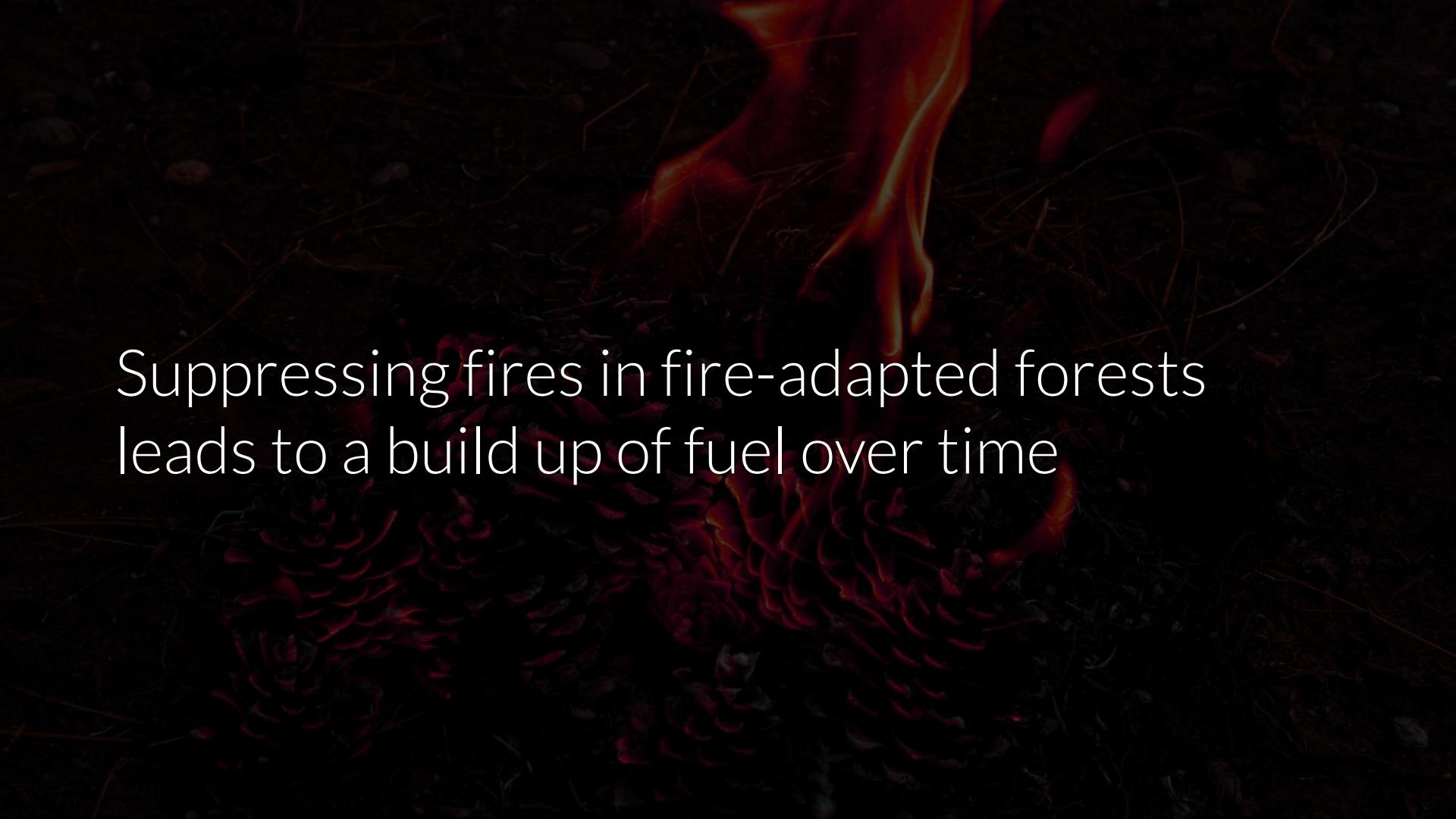
Robustness



Robustness: withstanding and resisting
a.k.a. “engineering resilience”

Safe development paradox: stability allows risk to accumulate, compromising resilience

Focus on just engineering resilience leads to
a maladaptive feedback loop



Suppressing fires in fire-adapted forests
leads to a build up of fuel over time

Patching & retroactive hardening of vuln-prone systems **accumulates risk**



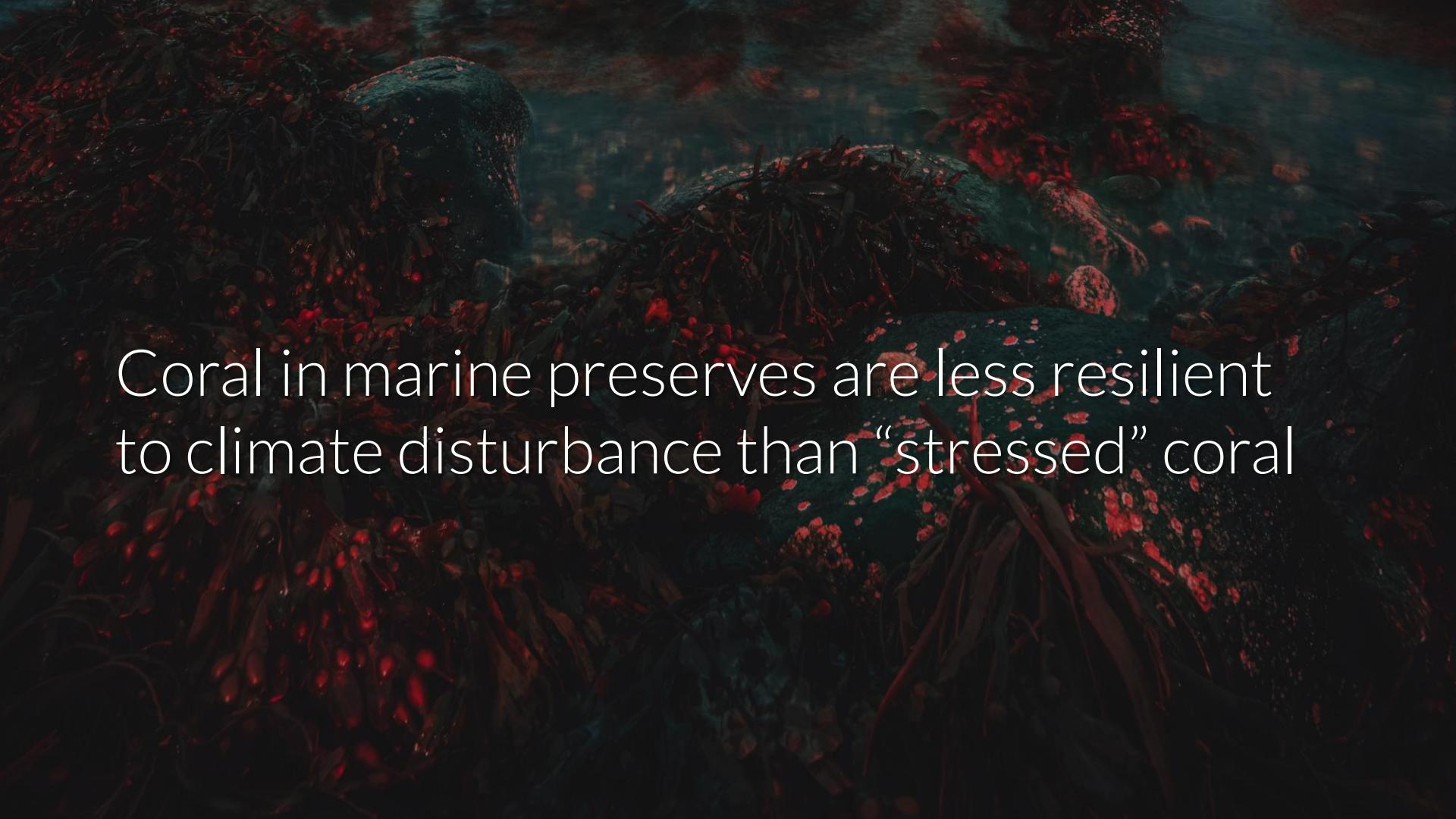
Levees support further human development
in at-risk floodplains



“Don’t treat the symptoms of bad planning
with structures”

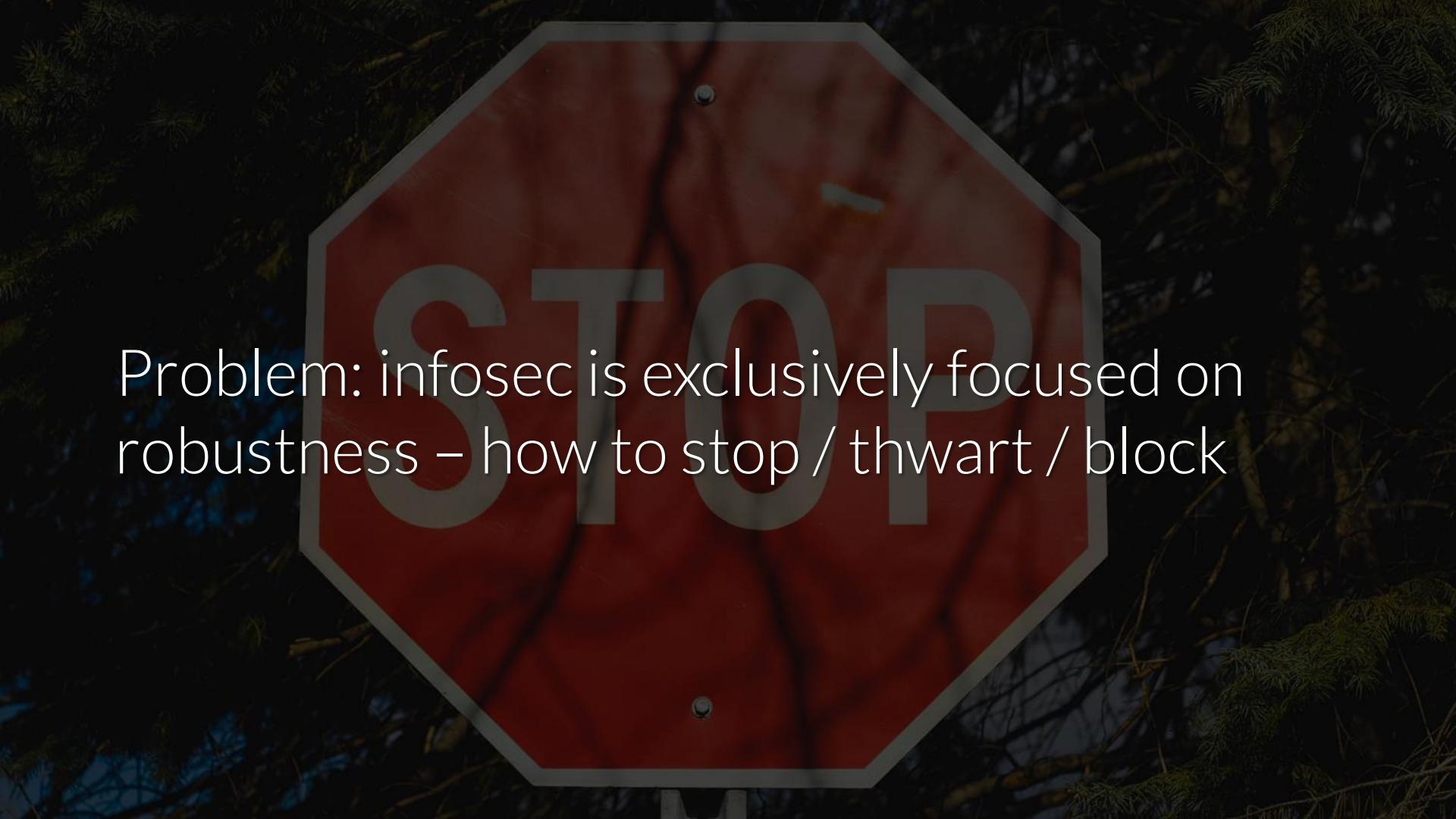
Technical controls shouldn't allow exemption from cyber insurance requirements

Artificially creating a stable environment
makes the system less adaptive to disruption



Coral in marine preserves are less resilient
to climate disturbance than “stressed” coral

Design & test internal systems with the same threat model as externally-exposed ones



Problem: infosec is exclusively focused on robustness – how to stop / thwart / block

Infosec's current goal is to return to
“business as usual” post-breach.

There is no such thing.

Other domains tried defying nature – it
doesn't work

Your systems must survive even if users click on phishing links and download pdf.zip.exe's



Robustness is effective when you have
diverse and layered controls



NYC's excess heat guidelines: backup hybrid-power generators, heat-tolerant systems, window shades, high-performance glazing

Diversity helps provide redundancy in
uncertain conditions

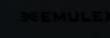
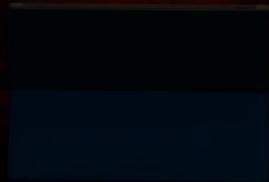
APT BlinkyBox™ doesn't help when legit
creds are used to access a cloud service

EMERSON
Control & Power

INEMULEX



Schneider

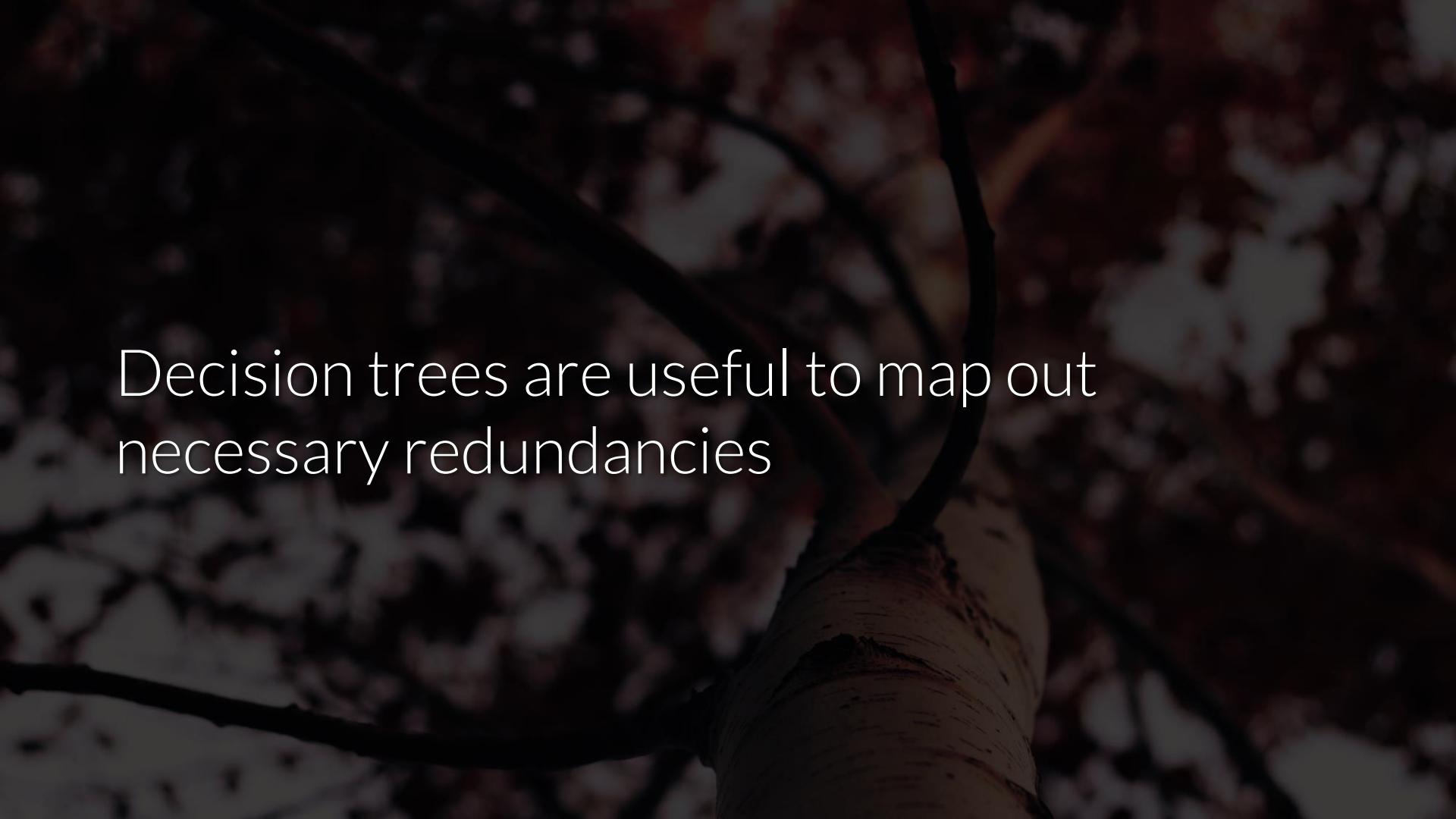


Don't ignore correlated risk.

Fragmentation can inject a healthy level of instability to foster resilience.

Pitfall of efficiency: more limited space in which your operations can survive

Up for debate: manageability via uniformity
vs. minimized impact via diversity?

A close-up photograph of a tree trunk, likely birch, showing dark, textured bark with some white lichen or moss. The lighting is dramatic, highlighting the texture of the bark.

Decision trees are useful to map out
necessary redundancies



Raising attacker cost is the bridge from robustness to adaptability

“Attackers will take the least cost path through an attack graph from their start node to their goal node.”

- Dino Dai Zovi

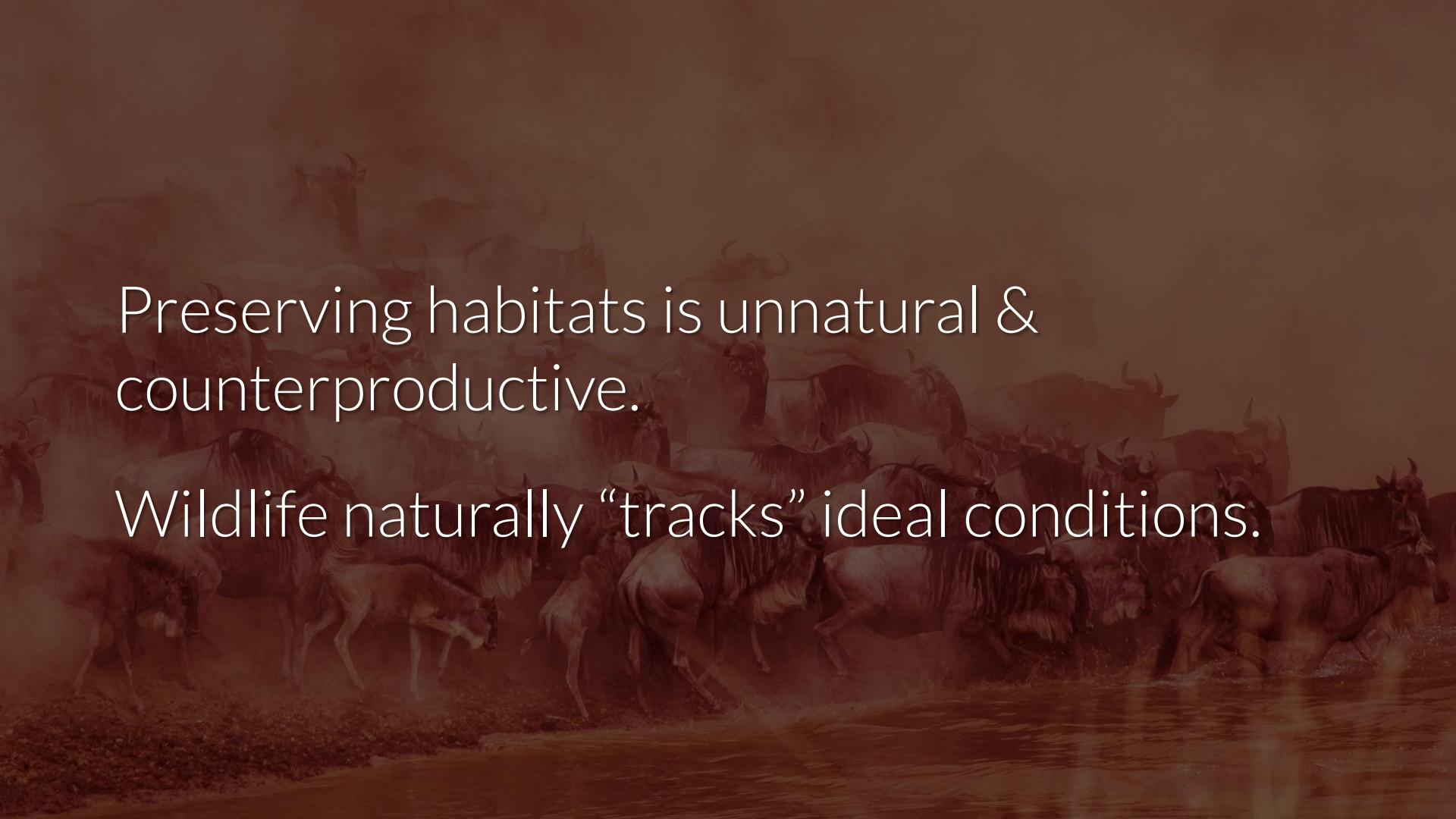


Adaptability

Adaptability: reduce costs and damage incurred, while keeping your options open

Intergov't Panel on Climate Change (IPCC):

Incremental change creates a false sense of security – goal is managed transformation

A dramatic photograph capturing a massive herd of wildebeests in mid-crossing of a river. The animals are moving from left to right, their bodies creating a dense, dark mass against a bright, hazy sky. Dust billows from their hooves, particularly visible in the lower left. The water in the foreground is turbulent and reflects the surrounding scene.

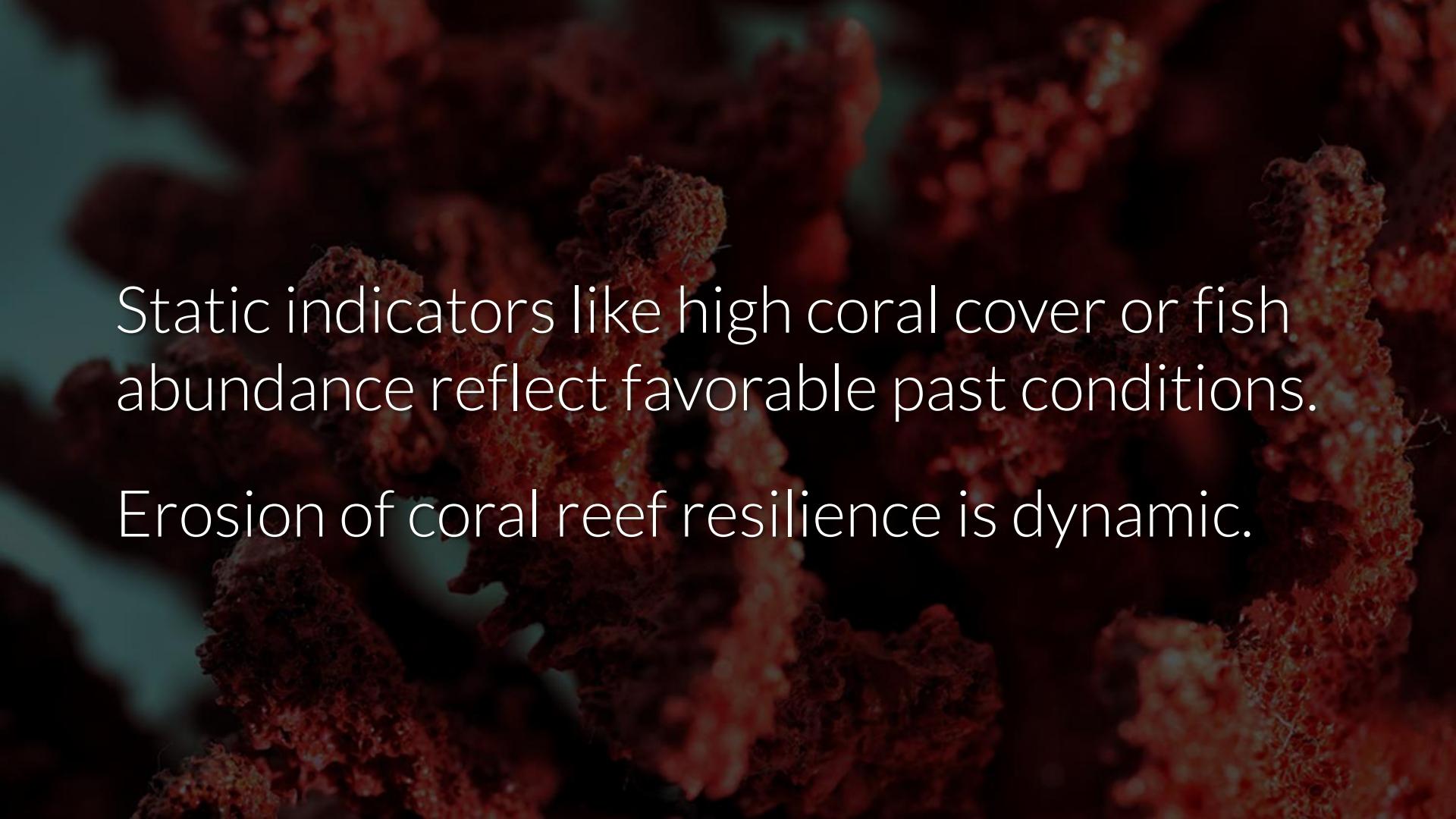
Preserving habitats is unnatural & counterproductive.

Wildlife naturally “tracks” ideal conditions.

Legacy systems are like preserved habitats.
We need to be able to migrate to better
conditions.

Example: patching inline PHP code

Instead: single class for DB queries

A close-up photograph of a coral reef. The corals are primarily orange and red, with some white and yellow patches. A small, light-colored fish is visible among the coral structures.

Static indicators like high coral cover or fish abundance reflect favorable past conditions.

Erosion of coral reef resilience is dynamic.

Ensure your threat models aren't based on favorable past conditions

A close-up photograph of a branch covered in frost, with several bright red rose hips visible against the white background.

Survival strategy: comingle warm-adapted species with cold-adapted cohorts

A dark, atmospheric photograph of a row of classic red British telephone booths lined up along a city street at night. The booths are illuminated from within, casting a warm glow through their glass windows. The word "TELEPHONE" is clearly visible above each booth's entrance.

Apps built with legacy systems and libs will
not survive in an increasingly open API world

Uncertainty and surprise must be baked into your approach

Test adaptability to attacker methods with
attack simulation or auto playbook testing

A close-up photograph of a monkey's face, focusing on the area around its eye and mouth. The skin is a vibrant red color with a distinct texture, possibly indicating a condition like rosacea or a specific breed trait. The surrounding fur is dark and dense.

Chaos Monkey

Randomly kills instances to test their ability to withstand failure.

It also makes persistence really hard.

Design your security architecture for survival even if individual controls fail

Rethinking security architecture is hard.

The industry offers too much complexity.



Containers



Containers promote adaptability and support transformability

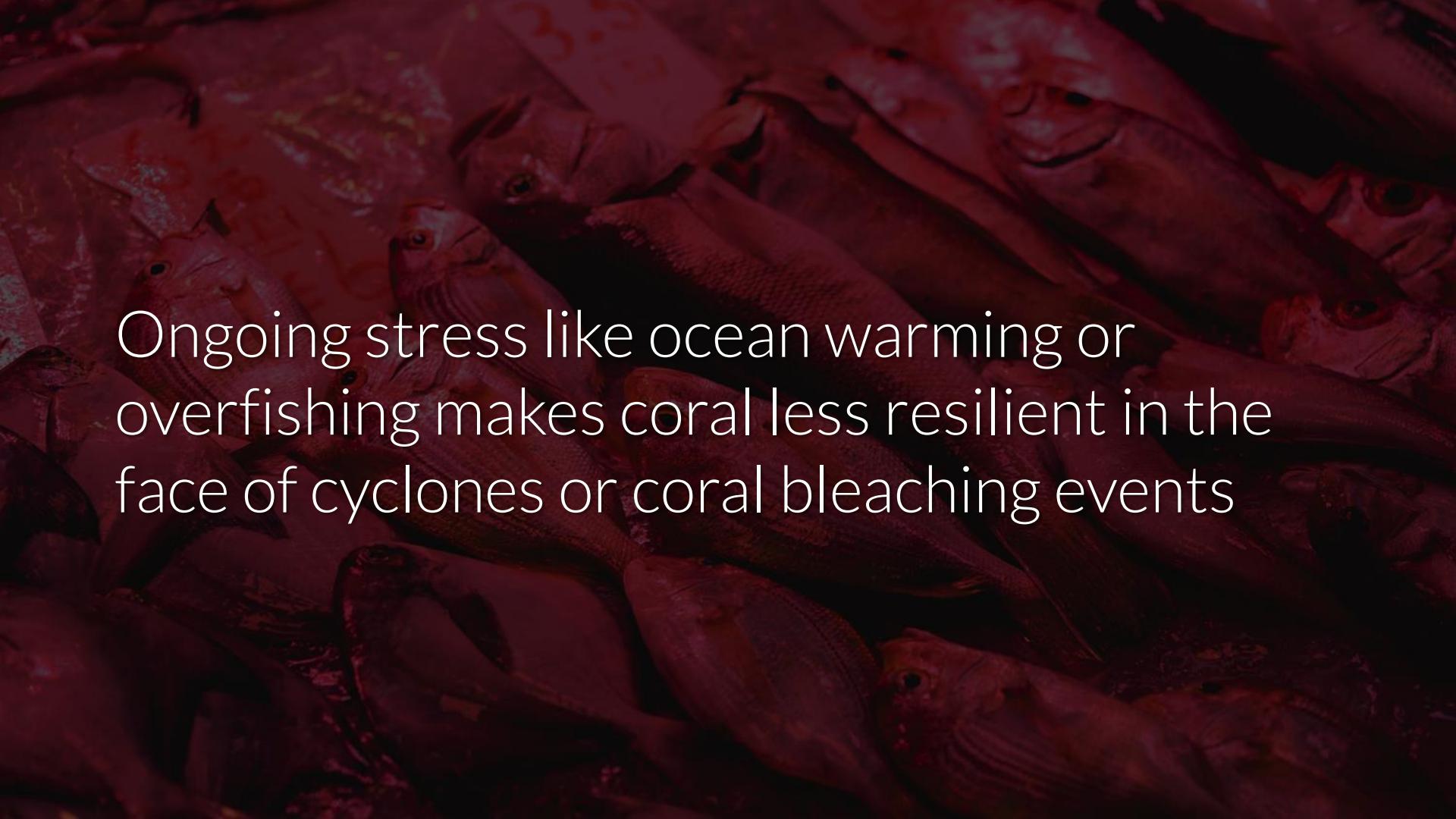
@jessfraz | blog.jessfraz.com/post/talks

Containers = “isolated, resource-controlled,
and portable runtime environments”

Easier to determine root cause

Easier to transport to better infrastructure

Easier to kill the infection & stop spread

A vibrant underwater photograph of a coral reef. Various species of fish, including a large school of yellowtail fusilier (Caesio terpsichore) and other smaller reef fish, are visible against a backdrop of intricate coral structures.

Ongoing stress like ocean warming or overfishing makes coral less resilient in the face of cyclones or coral bleaching events

Complexity will erode your resilience in the face of new vulns or data breaches



Transformability

Transformability = challenge existing assumptions & reorganize your system

Prior example: inline code makes it difficult
to reorganize your system vs. a single class



In disaster recovery policy, ideal is to change
location & remove urbanization

2011: 6.3mms earthquake hit Christchurch
Cost to rebuild of \$40bn+



NZ designated a “red zone” where land is too vulnerable & where rebuilding is uneconomic

Identify the red zones within your IT systems

Choose your own infosec redzone criteria:

Publicly exposed, legacy systems, critical data, privileged access, overly verbose, single point of failure, difficult to update, ...

Example: API consuming critical data should be in “red zone” whether it has vulns or not

Identify assets that fall under your red zone criteria & migrate them to a safer system

Example: Planned decommission of levees to assist migration

Prohibits becoming a permanent “fix”

A photograph showing a group of Maasai people, likely men, walking in a line across a dry, sandy landscape. They are wearing traditional red and blue shukas (wrap) and some have large circular beaded necklaces. Many are holding long wooden staffs or spears. The background shows sparse acacia trees under a clear sky.

Continually consider how you can prepare in advance for migration

A photograph of two women in an office setting. One woman, with dark curly hair and a white blouse, is smiling and looking towards the other. The second woman, with long dark hair and a red top, is also smiling and looking in the same direction. They are seated at a desk with a laptop between them. The background is blurred, showing office shelves and equipment.

Complex systems require collaborative
planning across stakeholders

Open sharing of protections in place, what risk remains, uncertainties in the approach

Partner with engineering – they benefit from flexibility and transformability as well



Your role is to manage state transitions.

Consider how a resilience approach fits into engineering workflows.

2FAC @ Facebook: integrated 2FA into dev workflows without creating friction



“You can actually implement security controls that affect every single thing people are doing and still make them love it in the process”

Find someone with whom to collaborate &
how security can fit into their workflows

Ensure your org is learning from prior experiences – foster a security culture

Conclusion

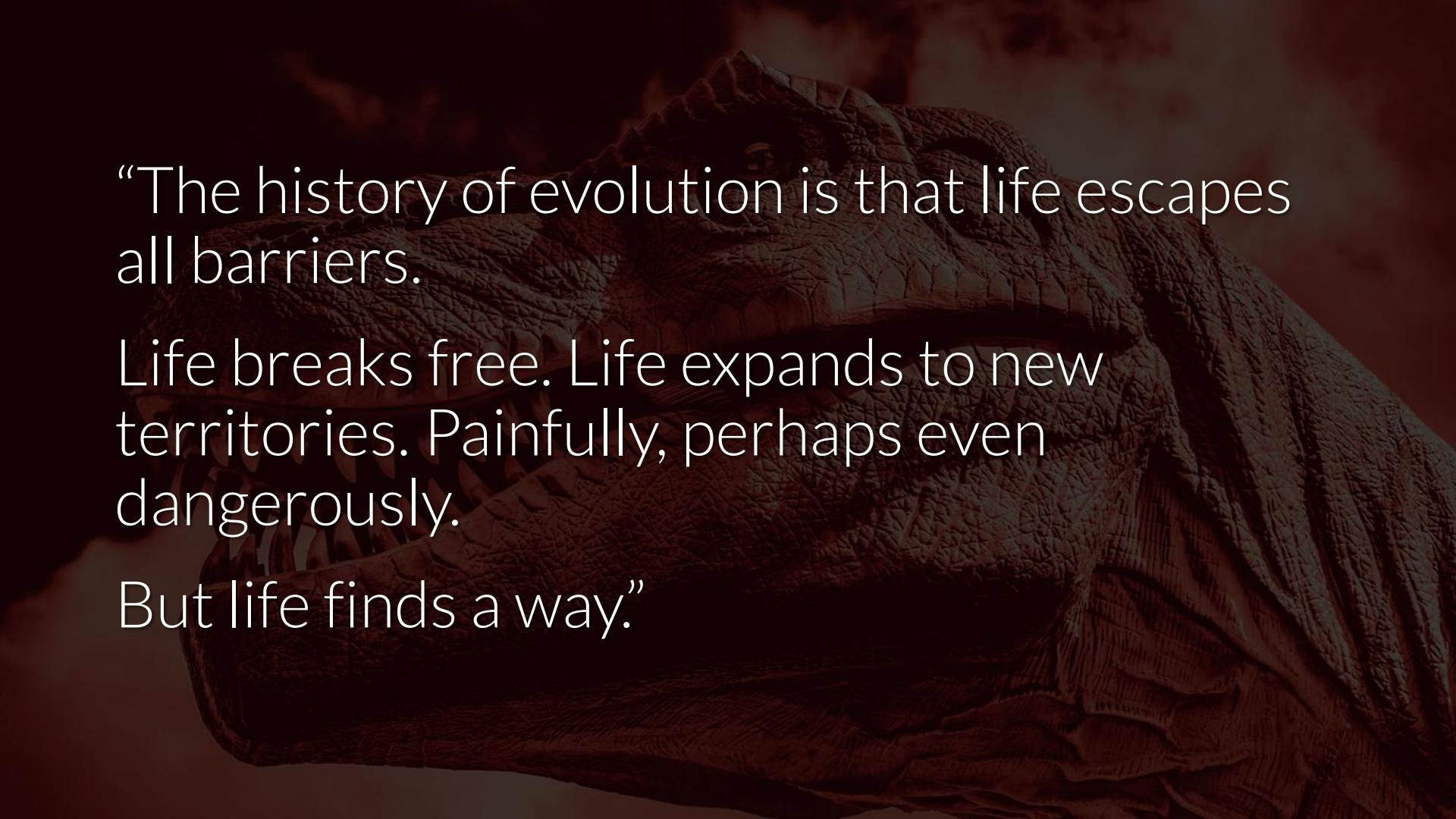


Infosec resilience means a **flexible** system
that can **absorb** an attack and reorganize
around the threat.

Robustness is optimized through diversity of controls

Adaptability minimizes the impact of an attack and keeps your options open

Transformability demands you challenge assumptions & reorganize around reality



“The history of evolution is that life escapes all barriers.

Life breaks free. Life expands to new territories. Painfully, perhaps even dangerously.

But life finds a way.”



Attacks will evolve. We can evolve, too.

Let's strive for acceptance of our grief, and
architect **effective** and **realistic** defense

A black and white cat is shown from the side, its head resting on a red surface. It wears a small, red, pointed hat with the words "FIRE CHIEF" printed on it in a stylized font. The background is dark and out of focus.

The blue pill relegates us to the role of a
firefighting cat who's drunk on snake oil

Instead of accepting snake oil, take the red
pill of resilience instead



“Good enough is good enough. Good enough always beats perfect.”

- Dan Geer



@swagitda_



/in/kellyshortridge



kelly@greywire.net

Suggested Reading

- Engineering resilience versus ecological resilience
- Resilience and disaster risk reduction: an etymological journey
- A strategy-based framework for assessing the flood resilience of cities – A Hamburg case study
- Vulnerability, Resilience, and the Collapse of Society
- Are some forms of resilience more sustainable than others?
- Flood Resilience: a Co-Evolutionary Approach
- The oak or the reed: how resilience theories are translated into disaster management policies
- Rethinking Ecosystem Resilience in the Face of Climate Change
- Building evolutionary resilience for conserving biodiversity under climate change
- Complexity and Planning: Systems, Assemblages and Simulations
- “[Windows Containers](#)” by Microsoft
- “[The Netflix Simian Army](#)” by Netflix