

The Red Pill of Resilience



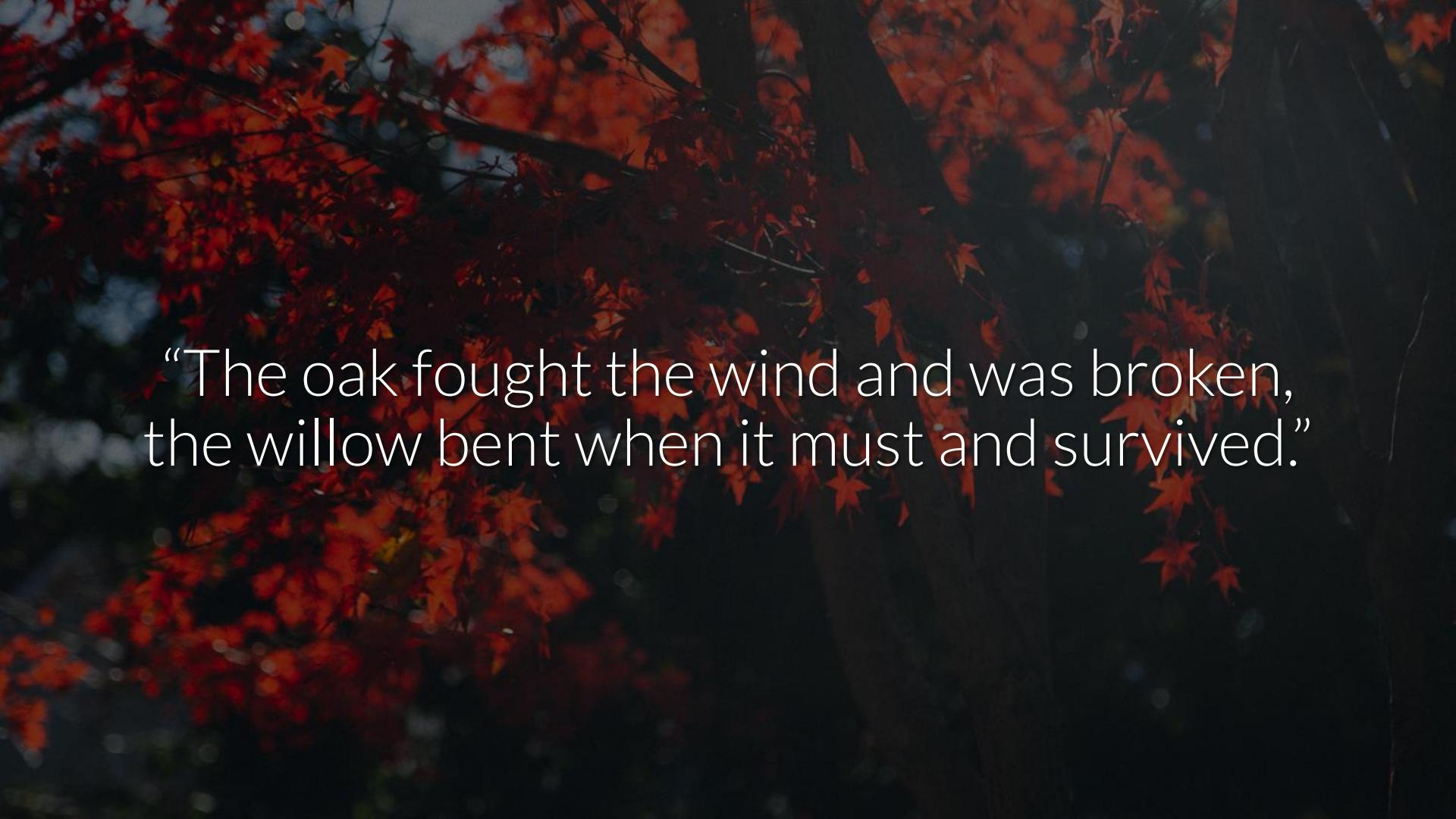
Kelly Shortridge (@swagitda_)
COUNTERMEASURE 2017

A gray tabby cat is sitting in a thick layer of fallen autumn leaves. The leaves are a mix of red, orange, yellow, and brown. The cat is facing away from the camera, its back and tail visible. It appears to be looking towards the left side of the frame.

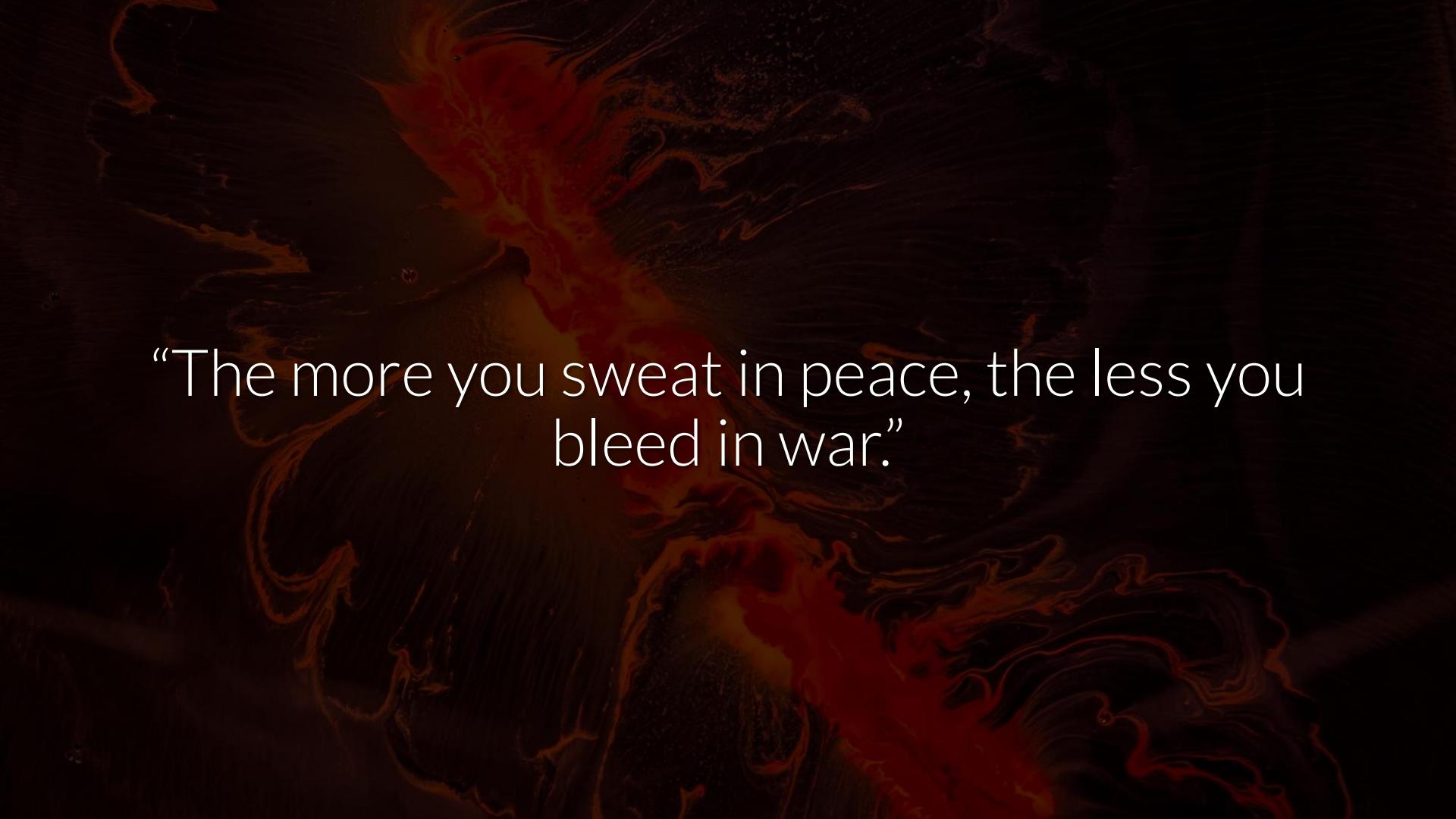
Hi, I'm Kelly



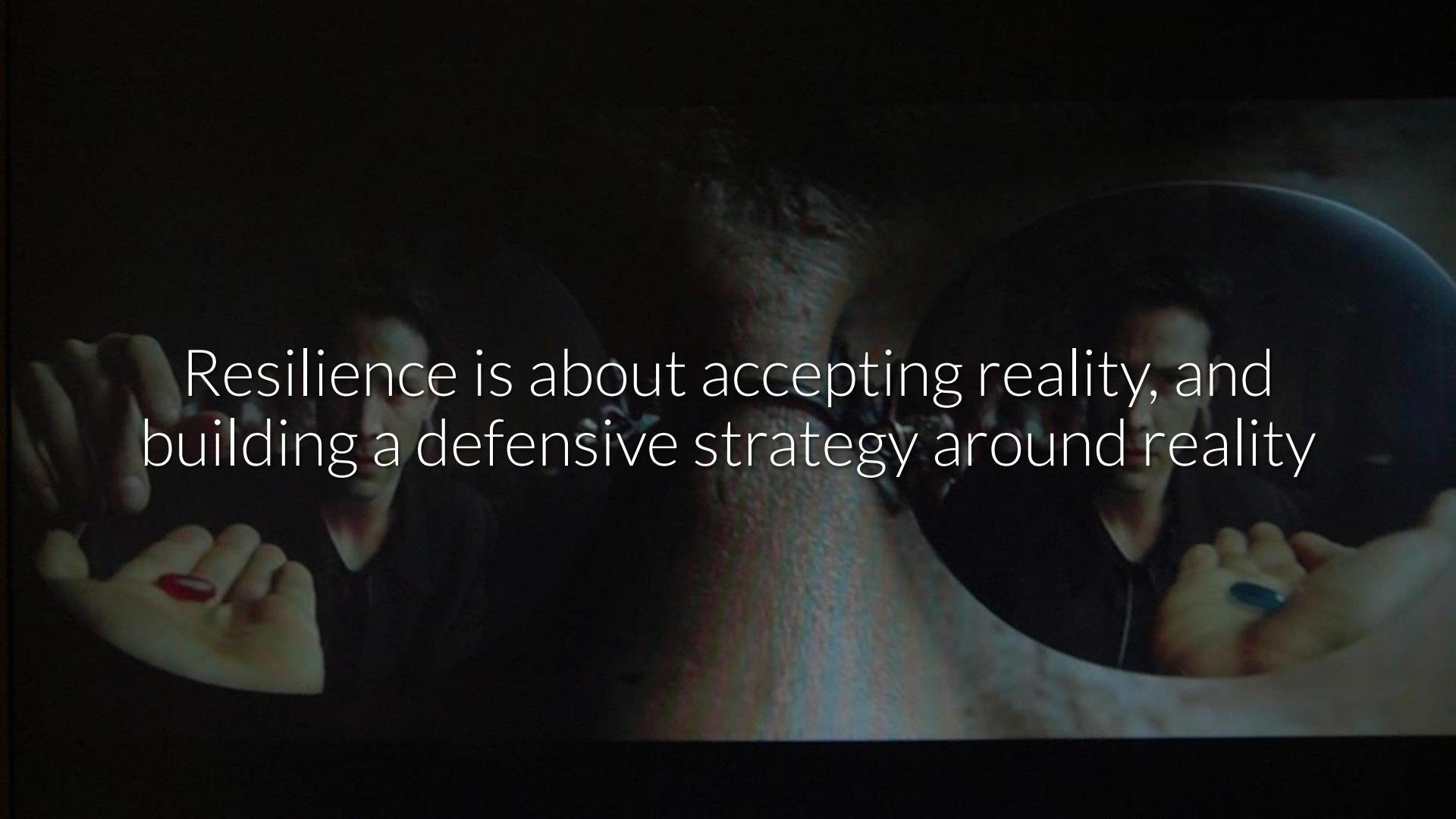
SecurityScorecard



“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.”



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 shows a dramatic, low-light scene of a mountain range. In the center, a sharp, snow-covered peak rises against a dark, overcast sky. The surrounding slopes are partially covered in snow and dark evergreen forests. In the immediate foreground, several trees are visible, their leaves a vibrant orange and red, suggesting autumn. 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

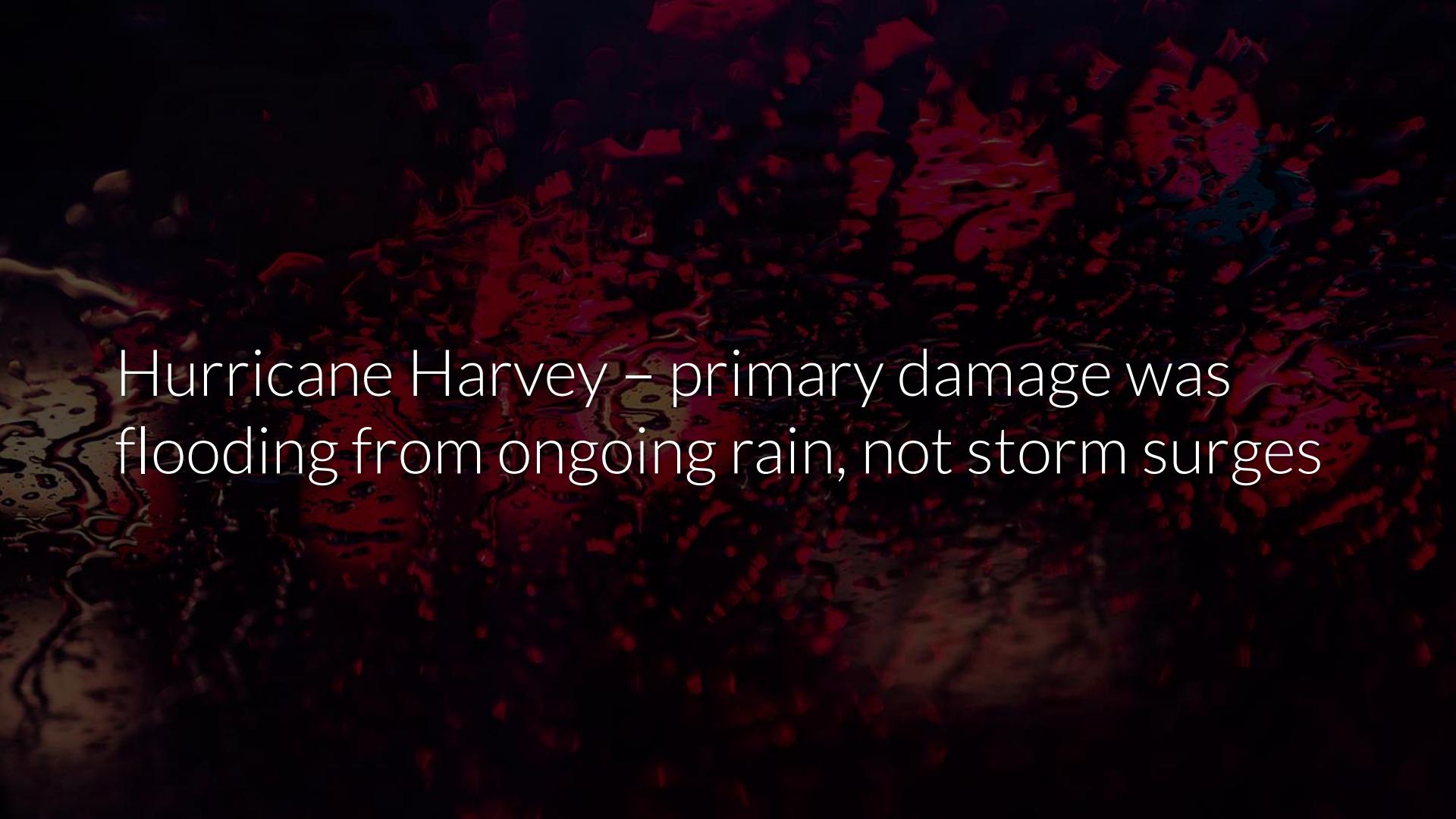
Evolutionary resilience assumes socio-ecological systems are co-evolutionary



Communities can diversify agricultural landscapes and production systems

Three central characteristics of resilience:

Robustness, Adaptability, Transformability



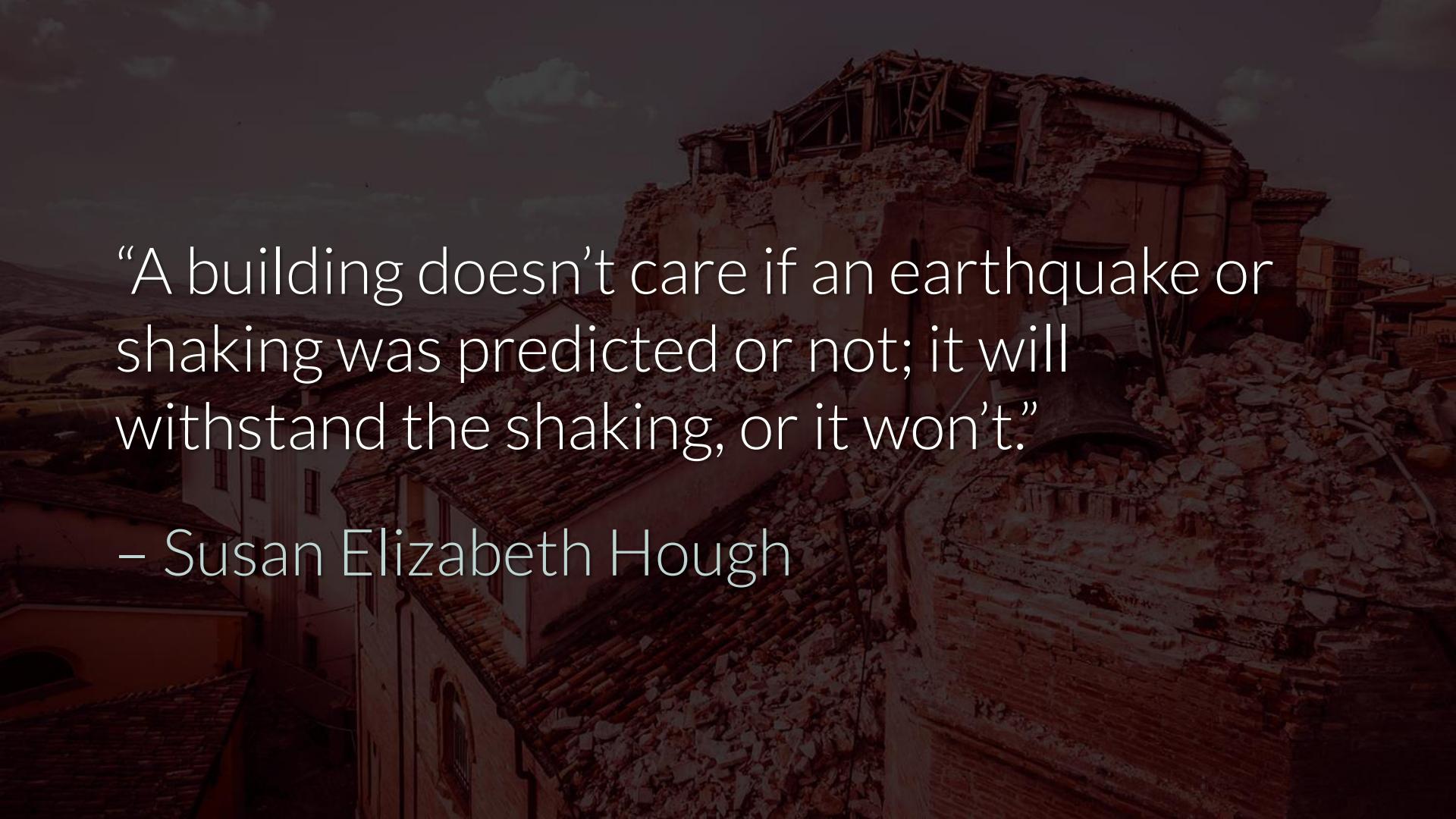
Hurricane Harvey – primary damage was flooding from ongoing rain, not storm surges

A photograph of a traditional Japanese garden path at night. The path is paved with rectangular stones and leads into the distance, flanked by a low wall on the left and a row of red torii gates on the right. A single traditional lantern hangs from a post on the right side of the path. The sky above is dark and filled with numerous small, glowing stars.

Resilience is about the journey, not the destination

Accept the risk will exist

Reduce potential damage & restructure
around the risk

A dark, somber photograph showing the aftermath of a disaster, likely an earthquake. In the foreground, a large, partially collapsed building with a tiled roof lies in ruins, its structure reduced to skeletal remains and piles of rubble. The surrounding area is filled with more debris and damaged buildings, under a heavy, overcast sky.

“A building doesn’t care if an earthquake or shaking was predicted or not; it will withstand the shaking, or it won’t.”

– Susan Elizabeth Hough

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

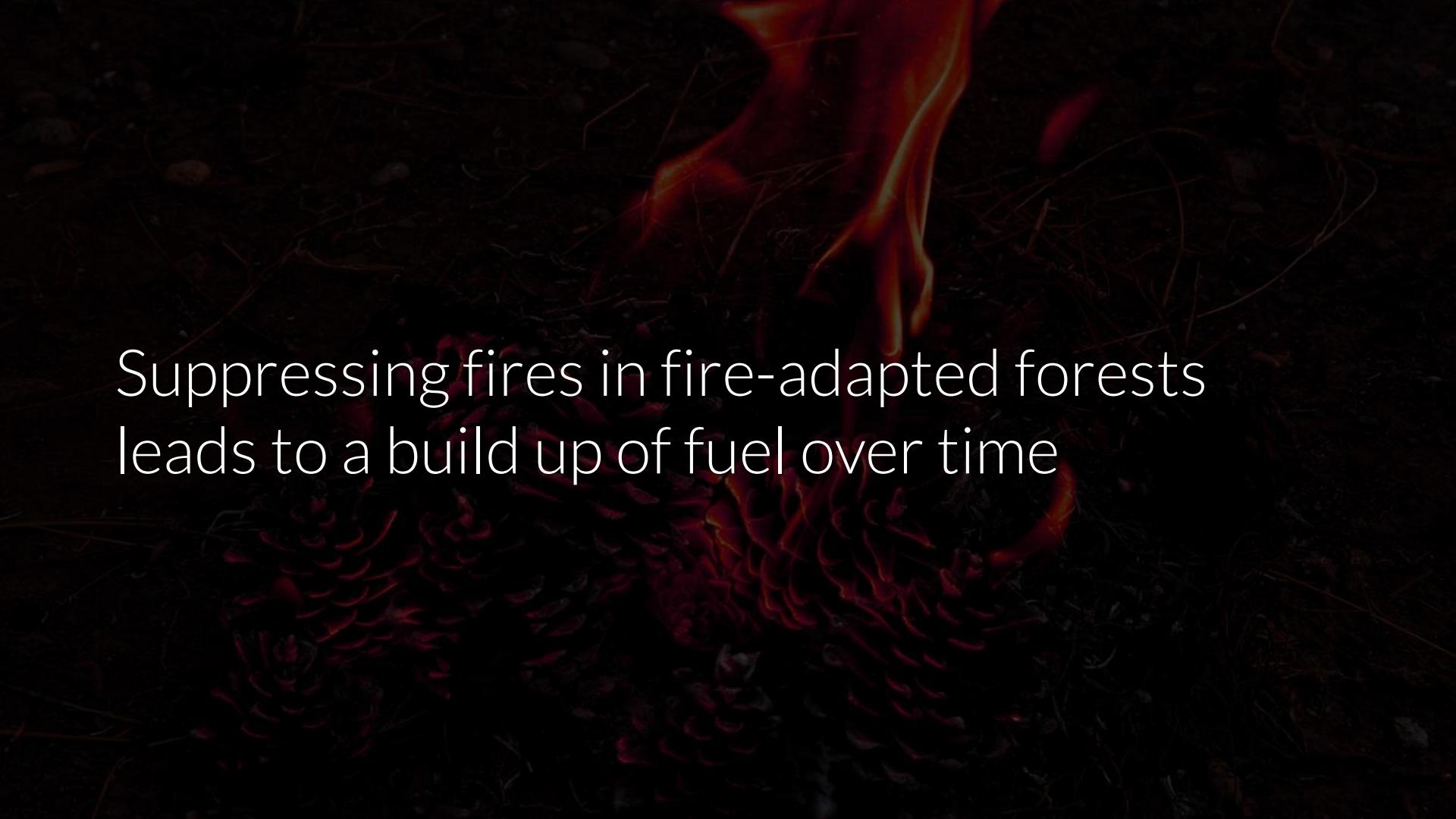
Robustness



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

The background of the slide is a dark, atmospheric photograph. In the lower-left foreground, a large pine cone is visible, its scales catching some light. Behind it, a fire burns, with bright orange and yellow flames rising against a dark, smoky background. The overall mood is somber and contemplative.

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

Patching & retroactive hardening of vuln-prone systems accumulates risk

A dark, grainy photograph showing a riverbank. In the foreground, there's dense, dark vegetation. A prominent, thick red wall, likely a levee or dam, runs horizontally across the middle ground. The water of the river is visible at the base of the levee, appearing dark and turbulent.

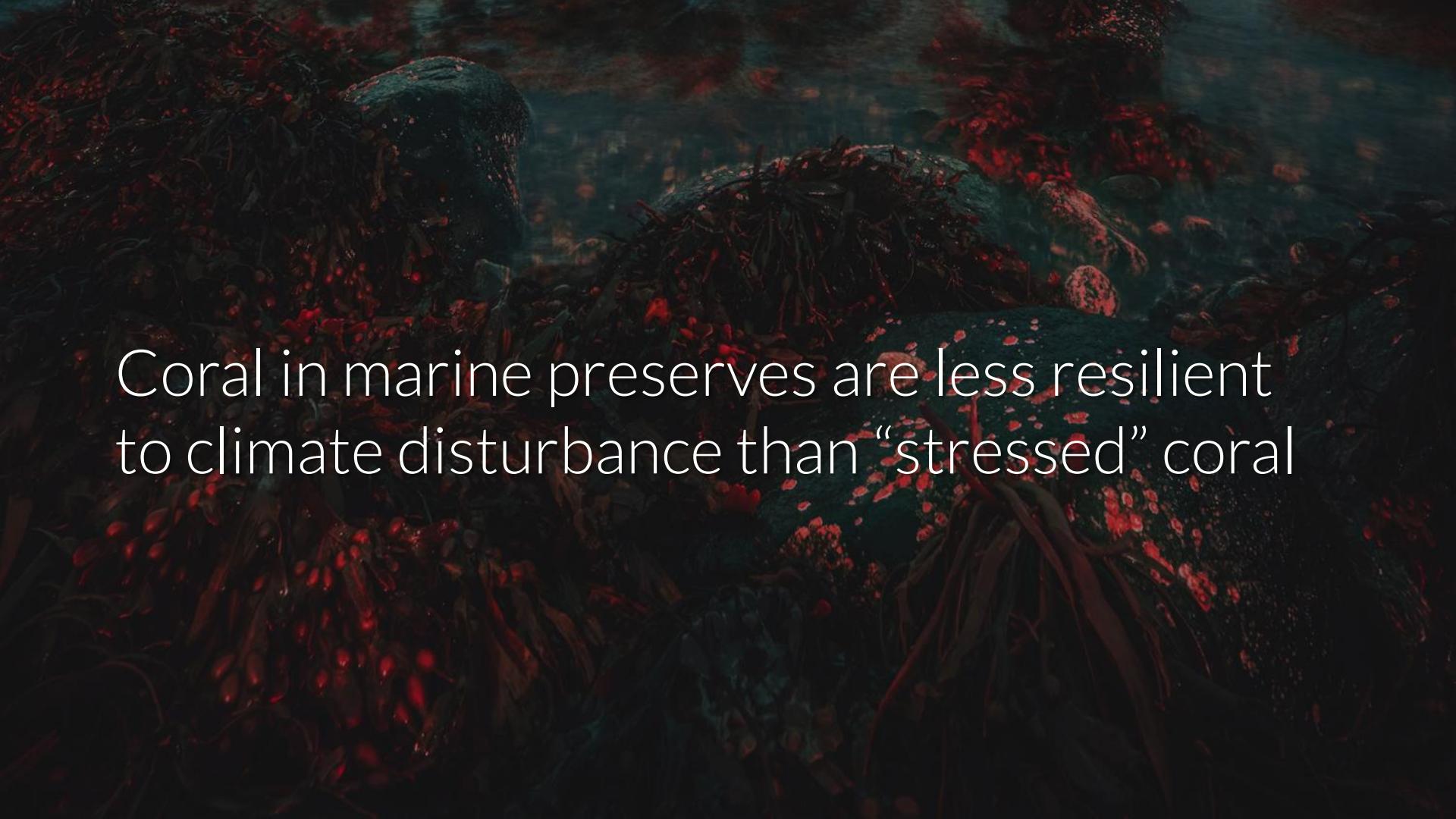
Levees support further human development
in at-risk floodplains



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

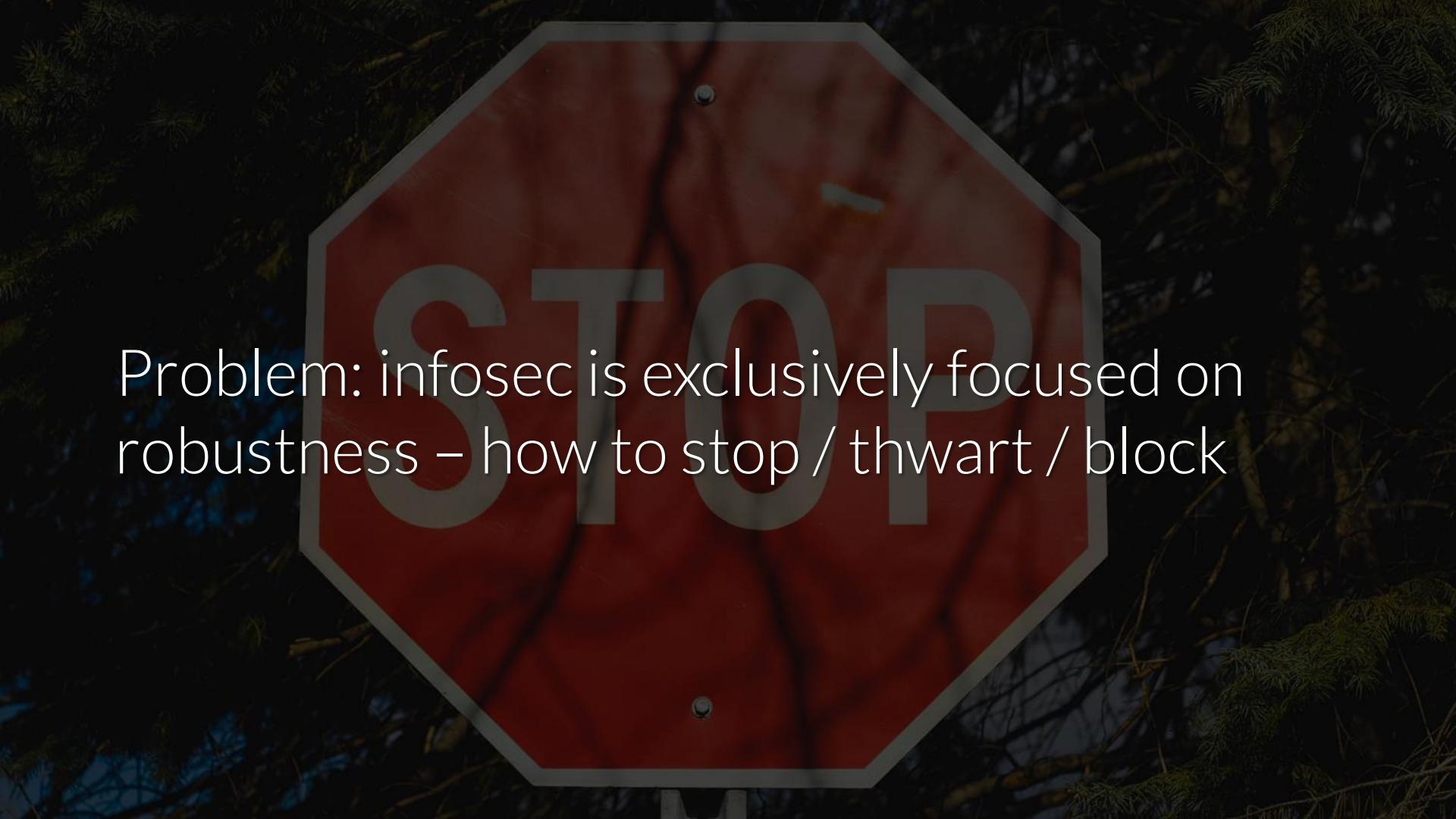
Technical controls shouldn't allow exemption from cyber insurance requirements

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

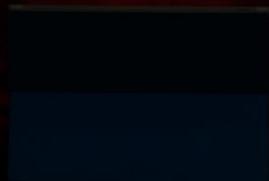
APT BlinkyBox™ doesn't help when legit
creds are used to access a cloud service

EMERSON
Control & Power

INEMULEX



Schneider

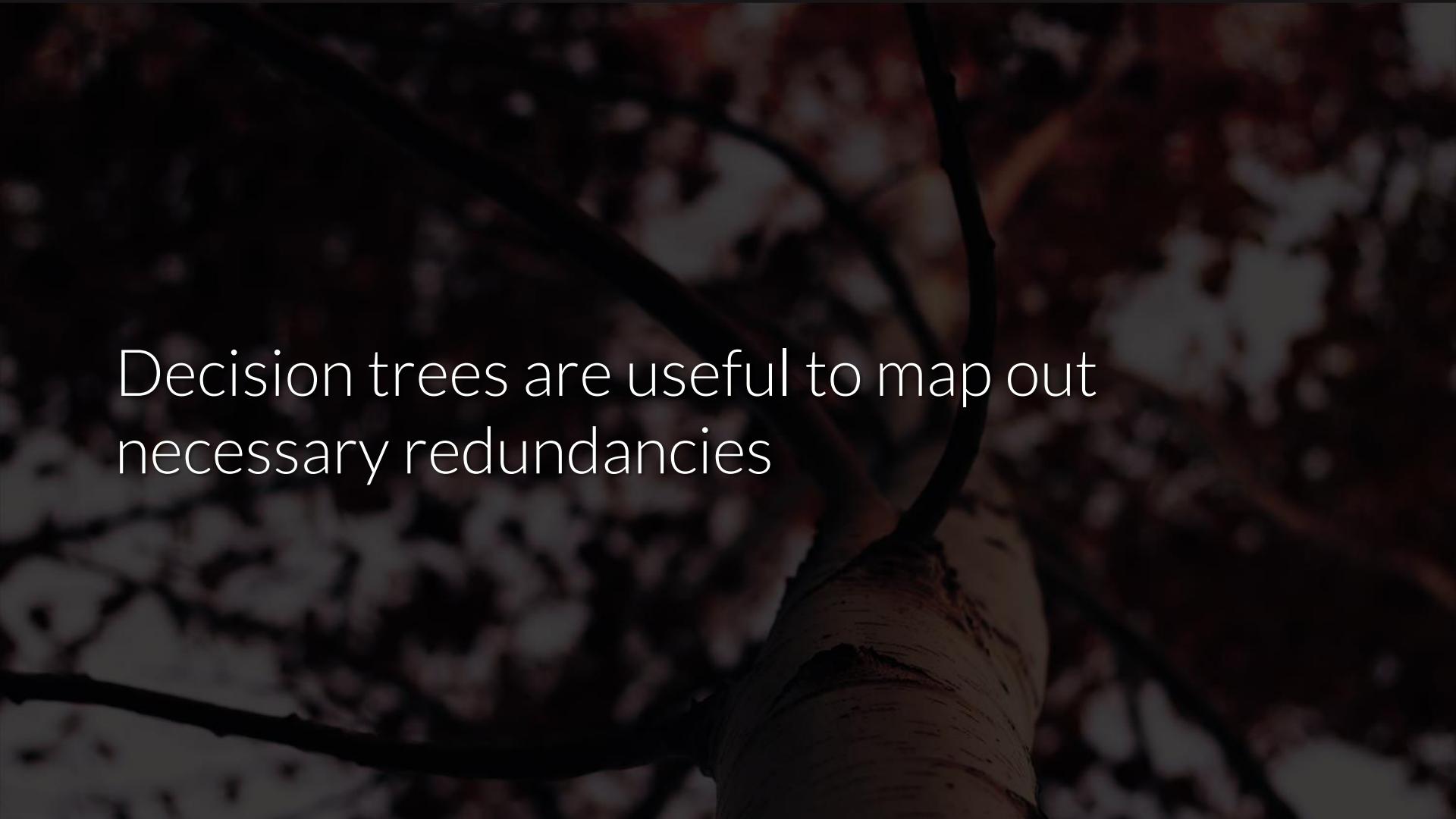


Don't ignore correlated risk.

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. The bark is dark brown with prominent, irregular ridges and grooves. Some light-colored, fuzzy growth, likely lichen or moss, is visible on the upper left side of the trunk.

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

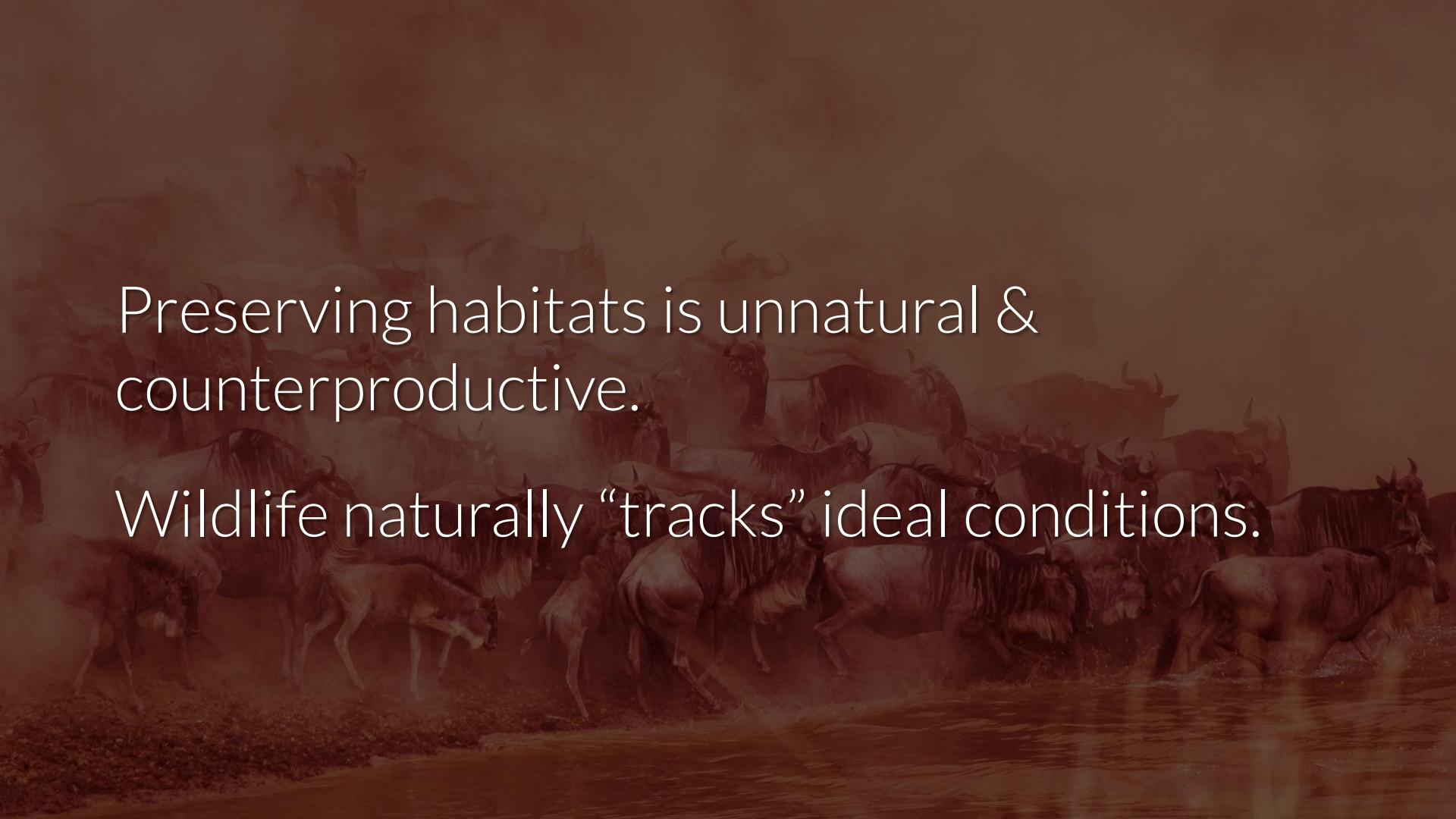


Adaptability

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.

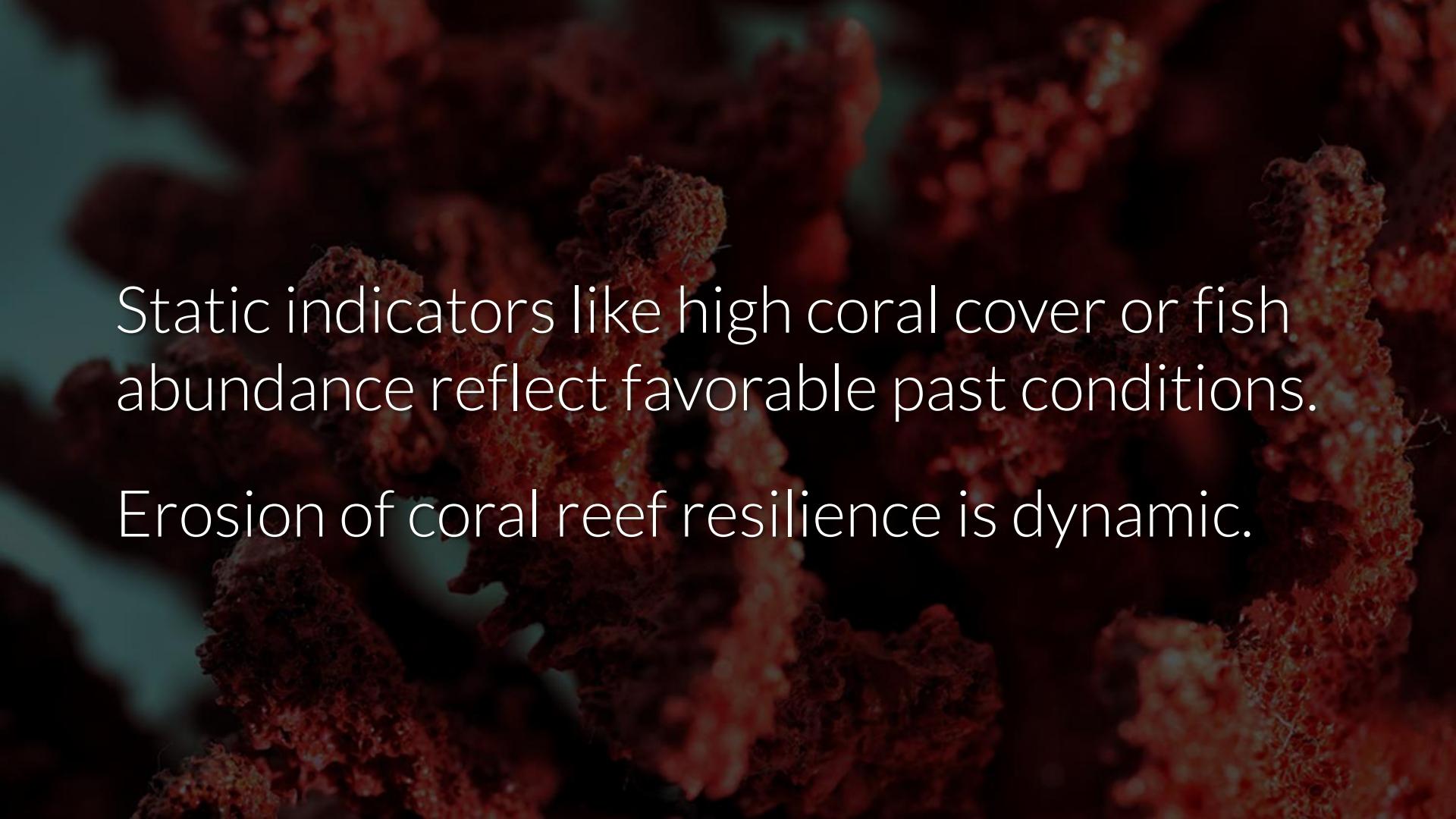
Preserving habitats is unnatural & counterproductive.

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



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

A dark, atmospheric photograph of a row of classic red British telephone boxes lined up along a city street at night. The boxes are illuminated from within, casting a warm glow through their glass windows. The word "TELEPHONE" is printed in white capital letters above each entrance. The scene is set against a backdrop of a large, multi-story brick building with visible windows and architectural details.

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



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

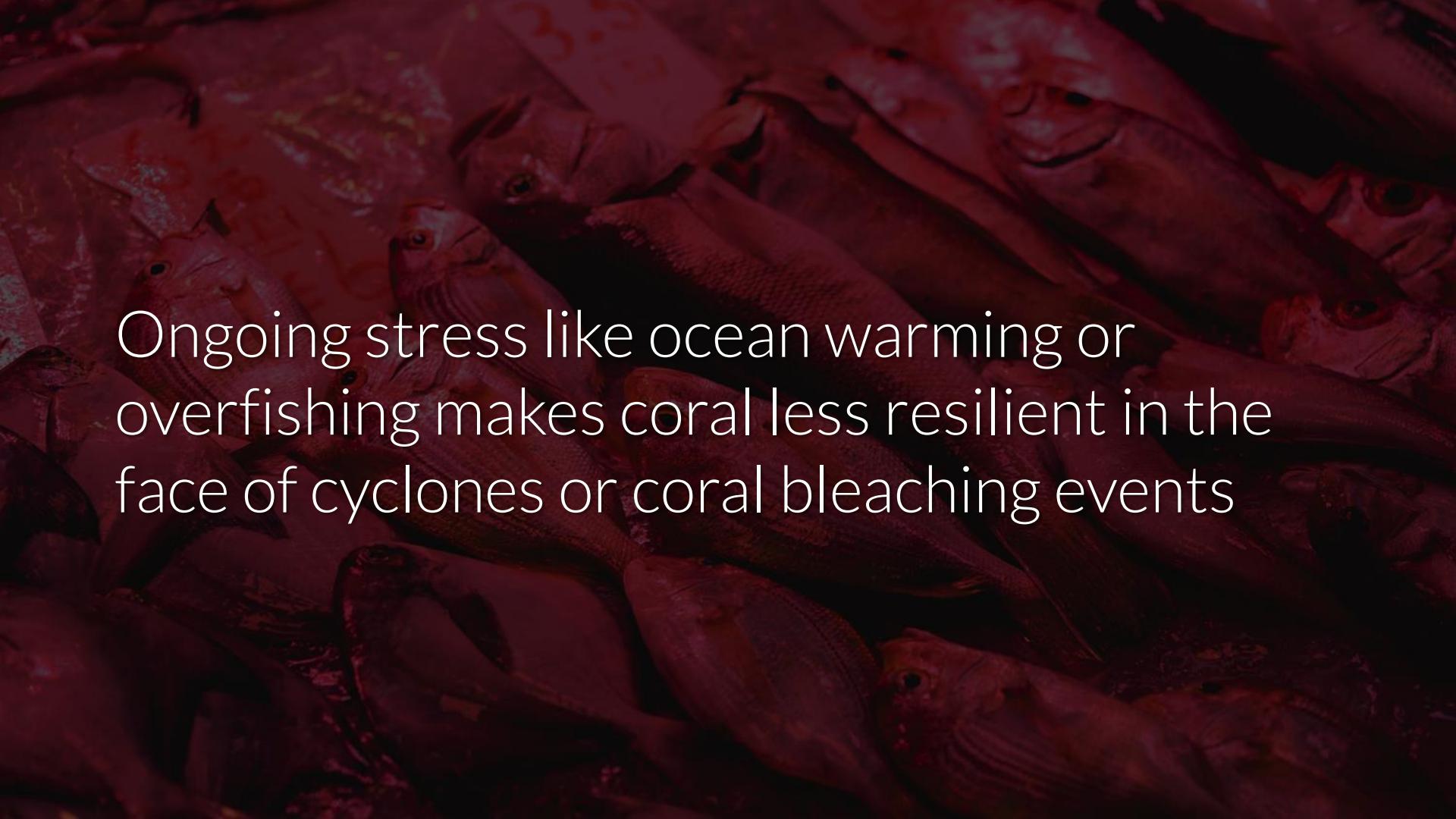
@jessfraz | blog.jessfraz.com/post/talks

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

Easier to determine root cause

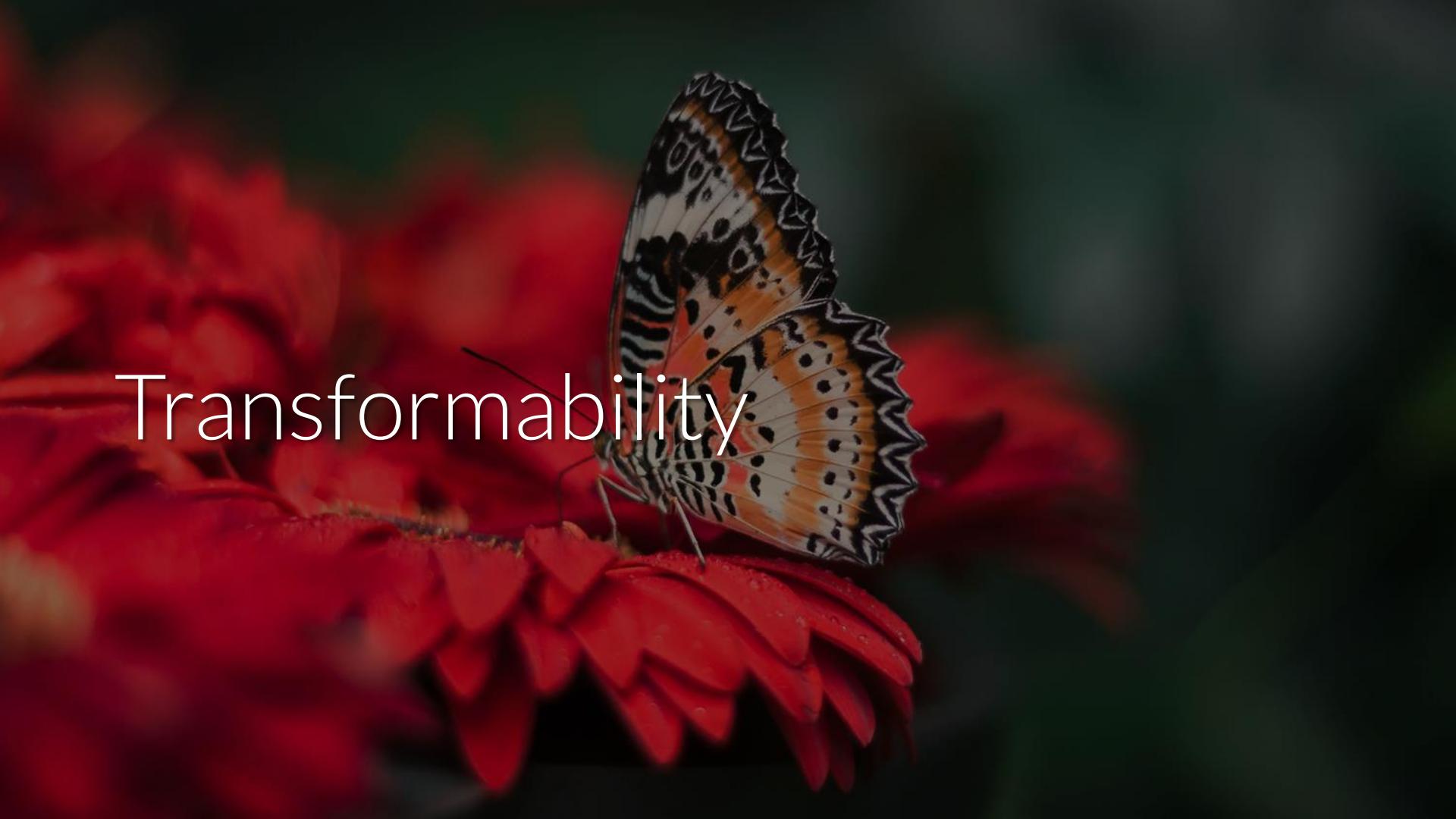
Easier to transport to better infrastructure

Easier to kill the infection & stop spread

A vibrant underwater photograph of a coral reef. Various tropical fish, including yellowtail fusiliers and damselfish, are visible among the coral structures. The water is clear, allowing for a detailed view of the marine life and the intricate textures of the coral.

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

A close-up photograph of a butterfly with patterned wings resting on a vibrant red flower. The background is dark and out of focus, making the red flower and the butterfly stand out. The butterfly's wings have intricate black, orange, and white patterns.

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+

A red rectangular sign with a white border and a large white exclamation mark symbol. The word "DANGER" is written in bold, white, sans-serif capital letters across the center of the sign. The sign is mounted on a metal railing, with visible bolts and a chain-link fence in the background.

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, both men and women, dressed in their traditional red and black shukas (wrap) and beaded necklaces. They are walking in a line across a dry, light-colored, cracked earth surface, likely a dry riverbed or a very dry savanna. In the background, there are some sparse, dry trees. The lighting suggests it might be late afternoon or early morning.

Continually consider how you can prepare in
advance for migration

A photograph of two women in a professional setting. On the left, a woman with dark hair in braids, wearing a white blouse, is smiling and looking towards the right. On the right, another woman with long dark hair, wearing a red top, is also smiling and looking towards the left. They appear to be engaged in a friendly conversation. The background is slightly blurred, showing what might be office equipment or a window.

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

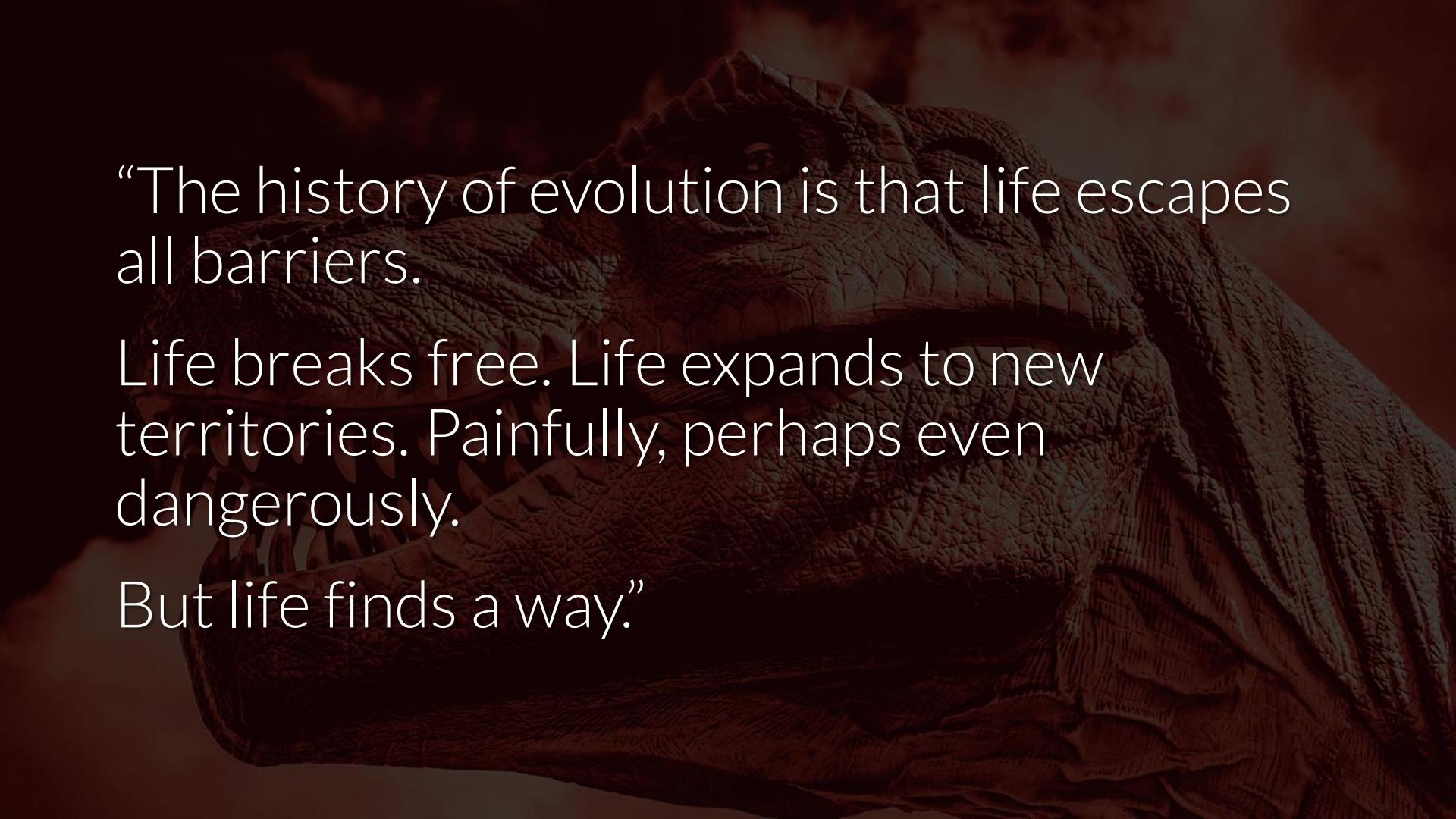


Infosec resilience means a **flexible** system
that can **absorb** an attack and reorganize
around the threat.

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 the central figure, lying down and looking slightly to the right. It wears a small, red, pointed cap with the words "FIRE CHIEF" printed on it in a serif font. The cap has a white border and a small emblem at the top. The cat's fur is dark with white patches on its chest and paws. In the background, a portion of a yellow fire hose is visible, along with some other indistinct elements of a firefighter's gear.

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