Security in design

Russ White

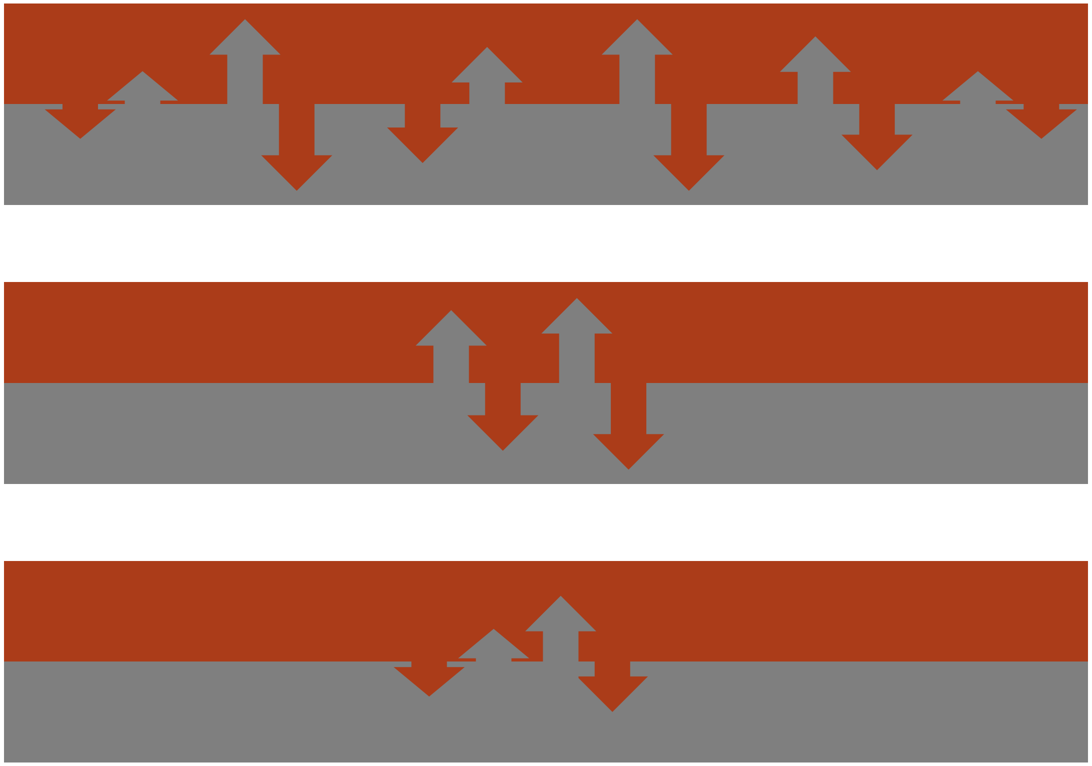
BUILD SECURITY IN FROM DAY ONE

but what does this mean?

Build Simple
Build Places for Policy
Build Measurable

The Internet and all the systems we build today are getting more complex at a rate that is faster than we are capable of matching. Security in reality is actually improving, but the target is constantly shifting. As complexity grows, we are losing ground.

Bruce Schneier
https://www.schneier.com/news/archives/2012/12/complexity_the_worst.html



Systems are bound together through interaction surfaces

Broader and Deeper

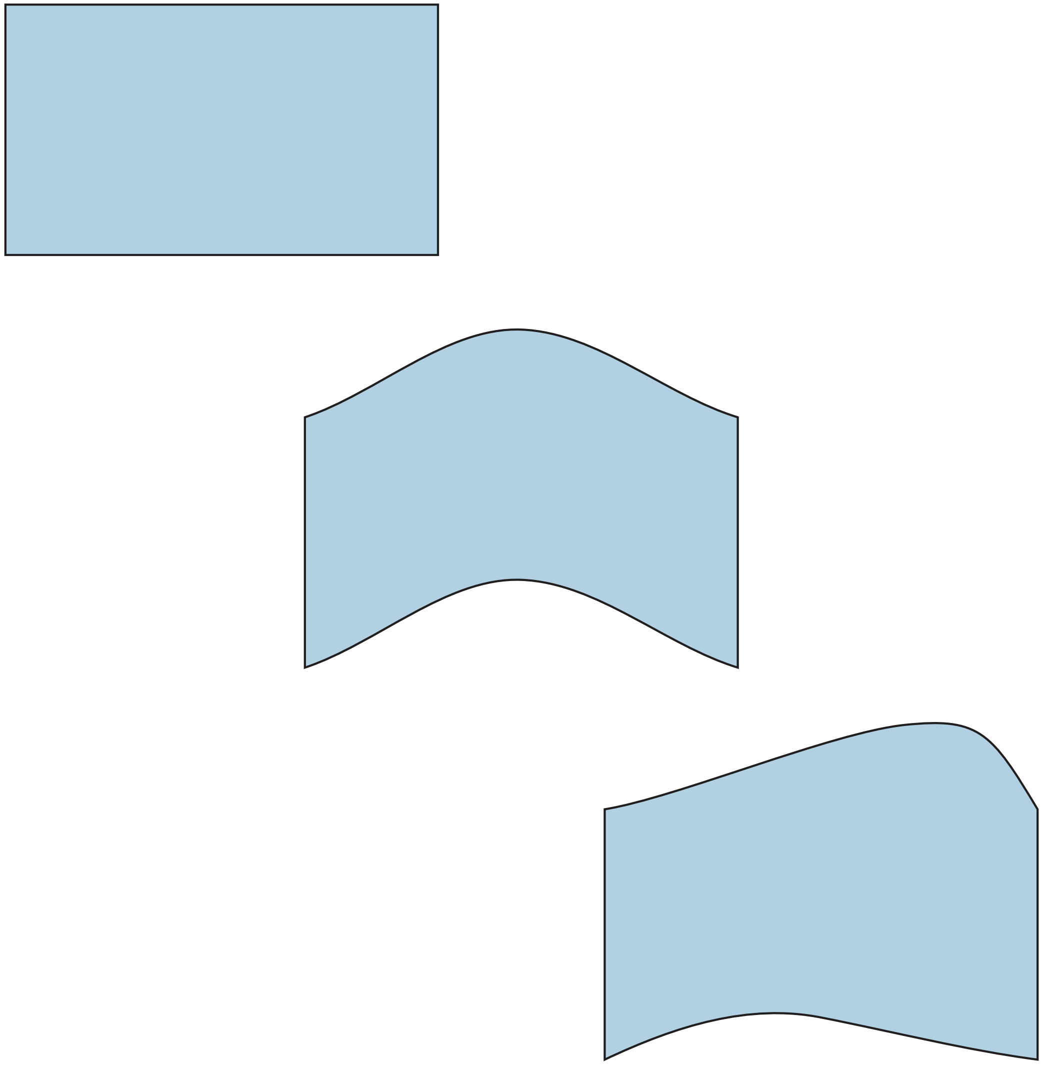
Tighter binding

Enables cross-system attacks

Larger and richer attack surface

interaction surfaces

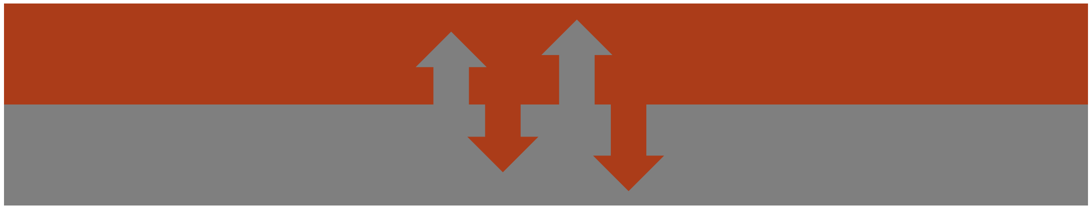
unintended consequences



Complexity increases unintended consequences

Unintended consequences are attack surfaces

Places for policy

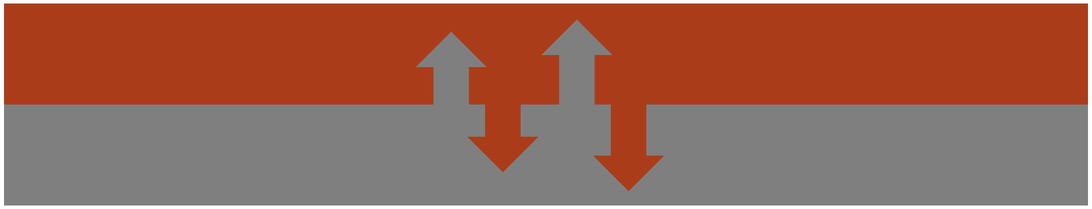


Policy containment is key to security

Either within a module or at an interaction surface

Subsidiarity Principle

places for measuring



Measurement requires context

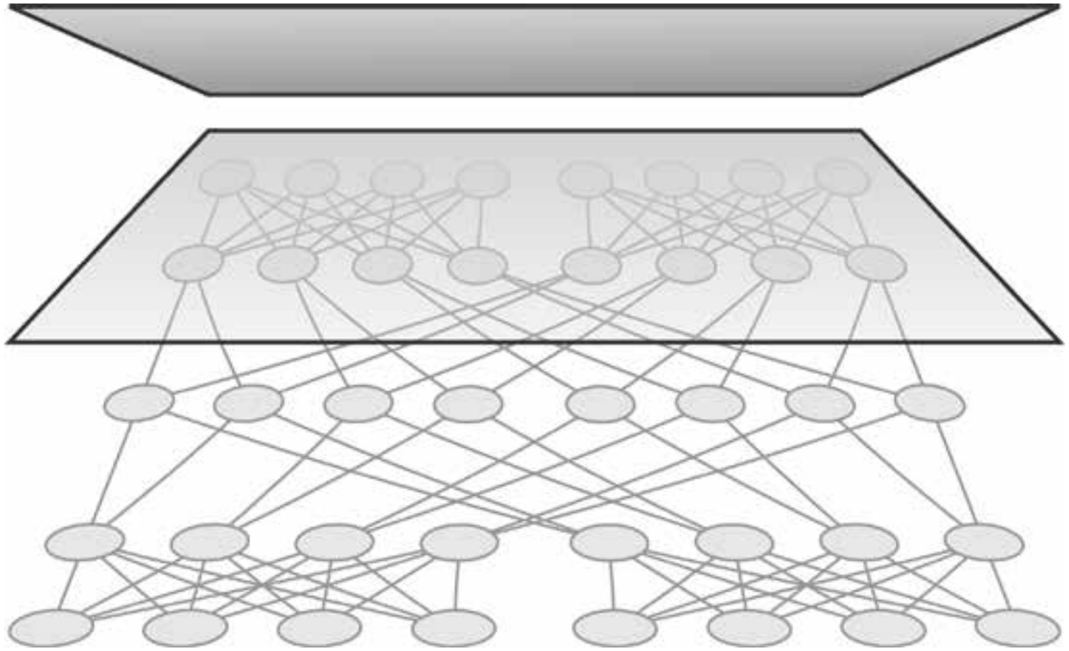
What normal looks like

Why normal looks that way (how this system works)

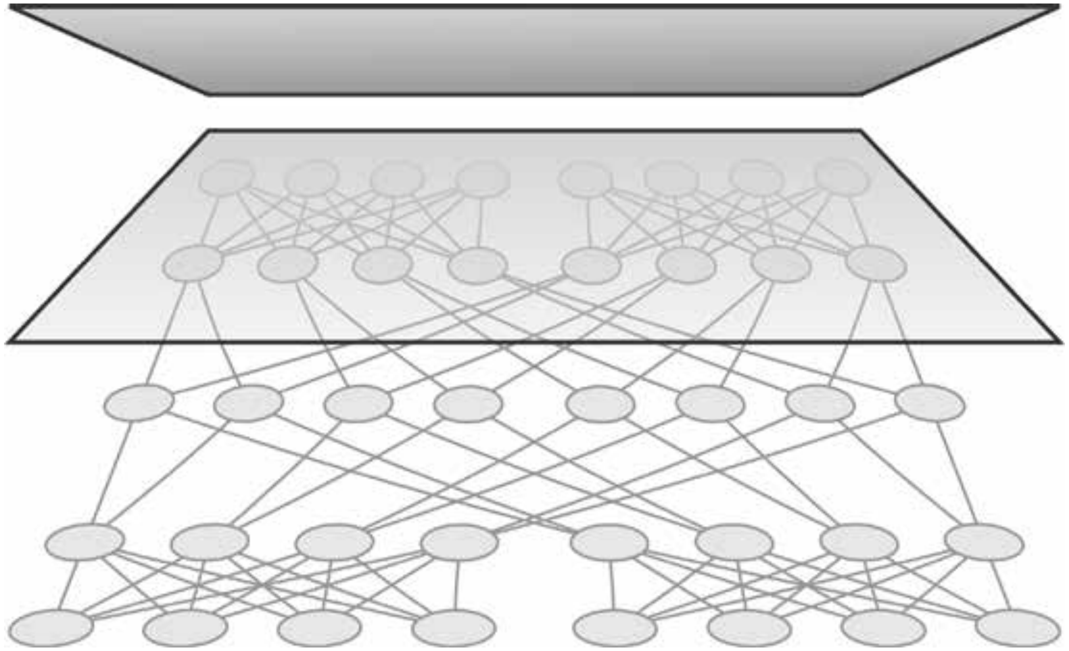
We normally reduce complexity via modularization

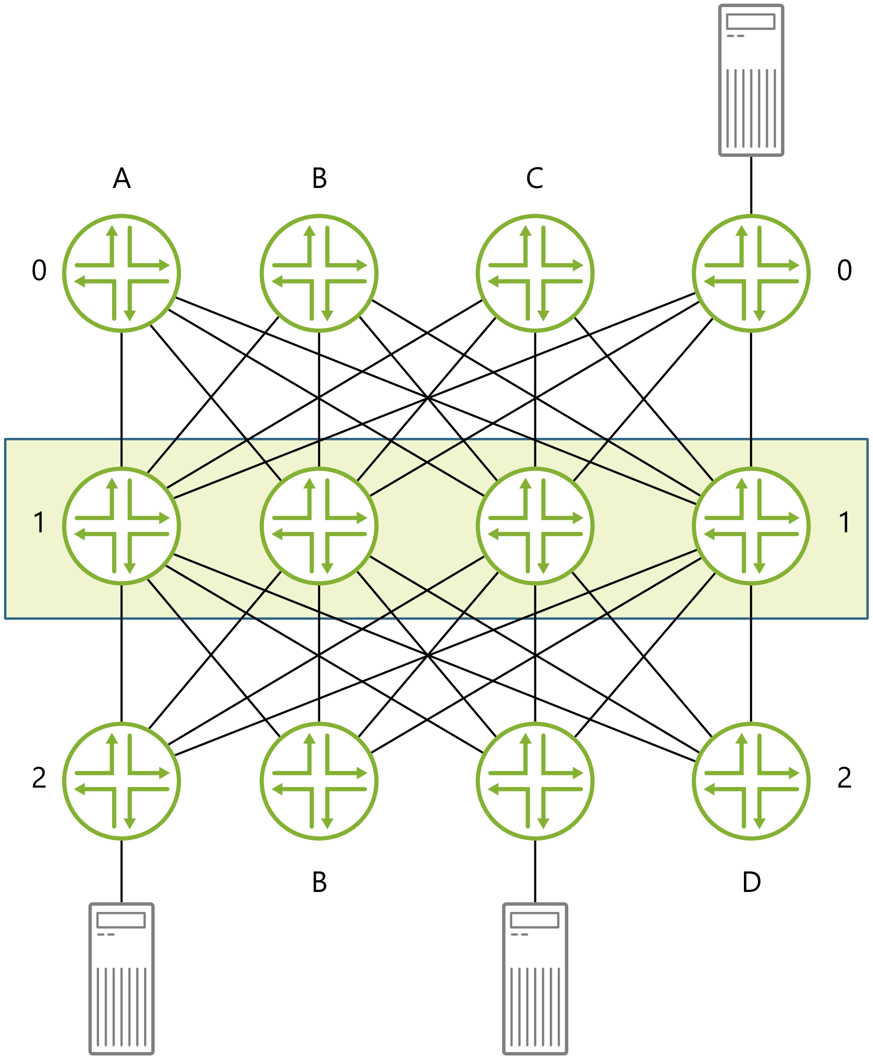
Modularization can also give us places for policy and places to measure

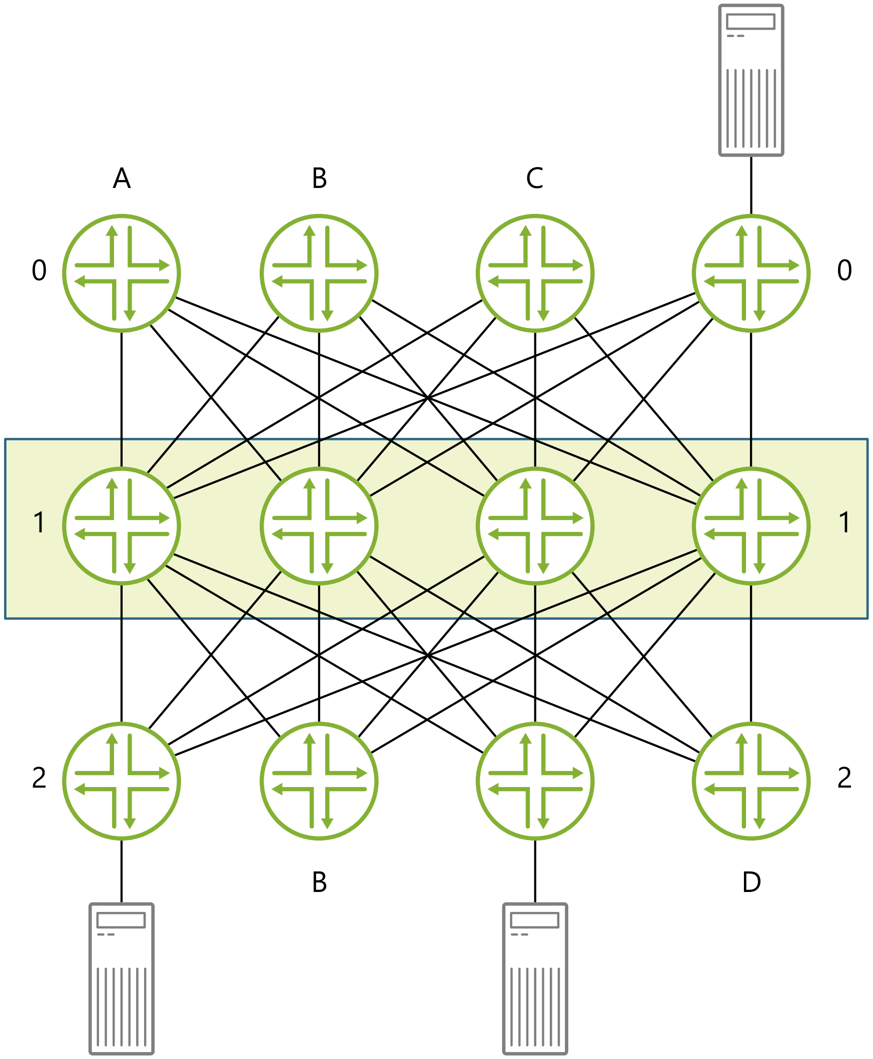
modules in a dc fabric



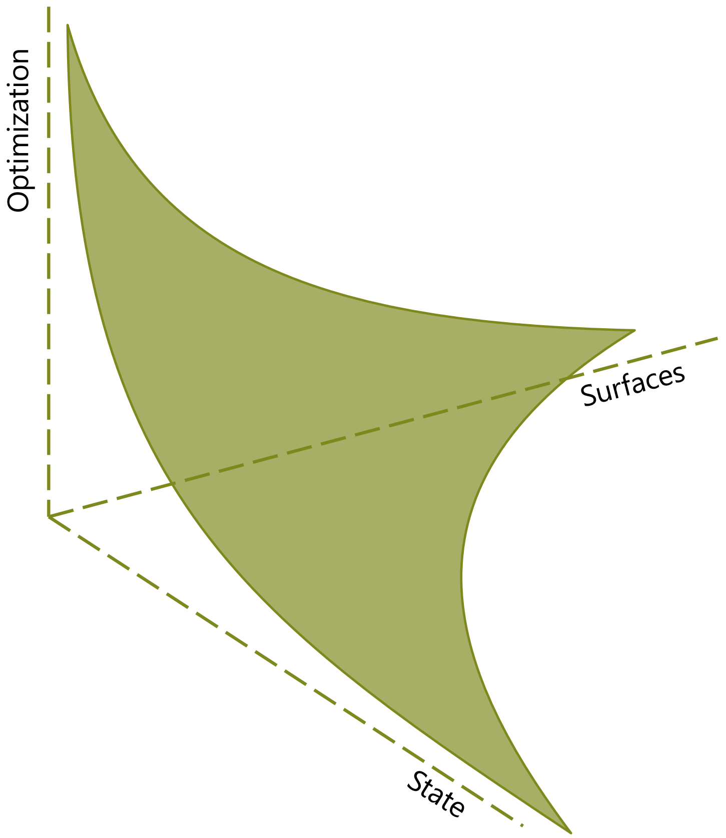
modules in a dc fabric




A
B
C
0
0
1
1
2
2
B
D


A
B
C
0
0
1
1
2
2
B
D

modularization tradeoffs



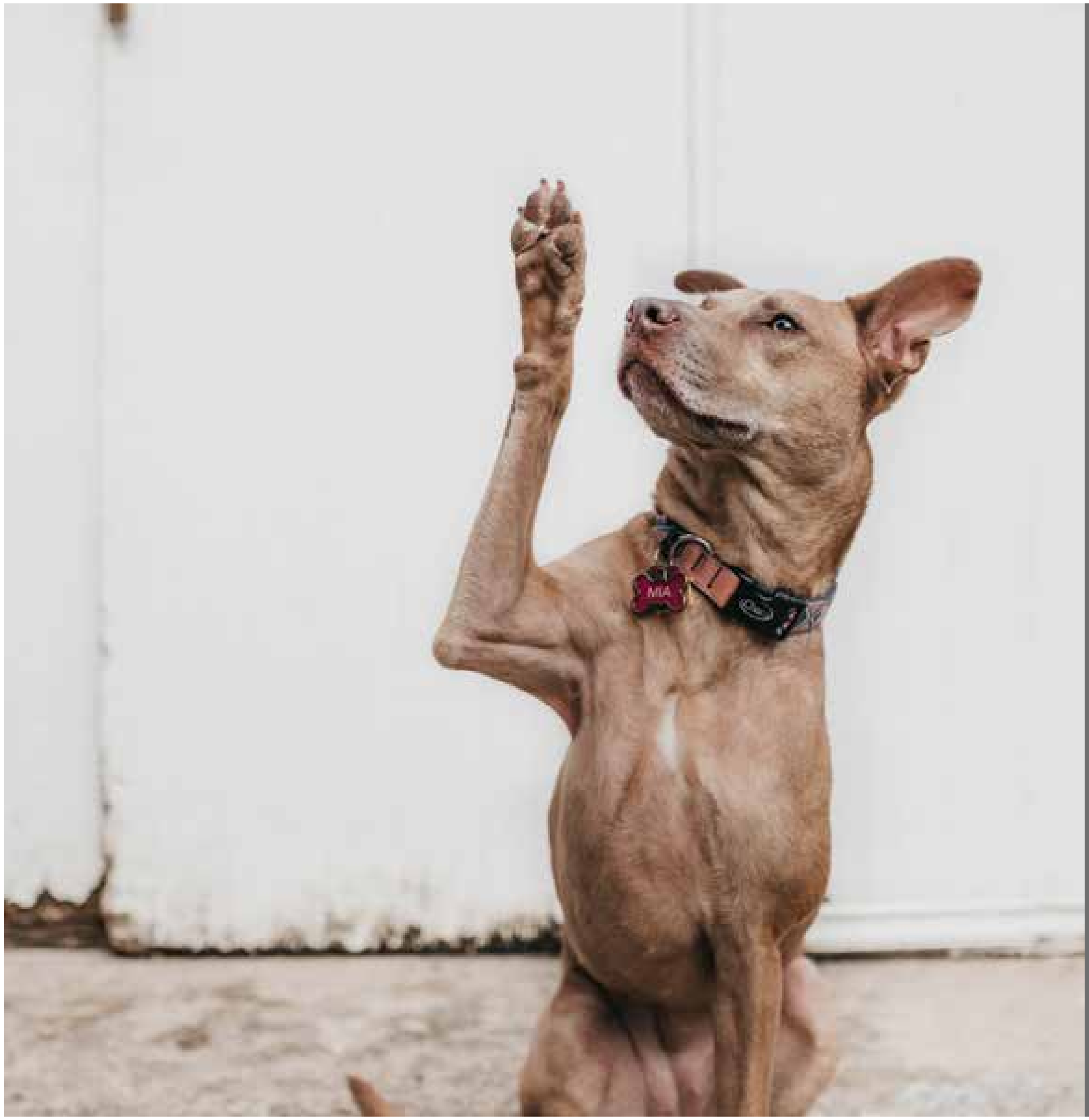
To optimize you either increase state or create new surfaces

Creating new surfaces and/or removing state almost always leads to less optimization

modularization tradeoffs

Reducing complexity locally almost always leads to increasing complexity globally

Optimizing locally almost always leads to decreasing optimization globally



RULE11·TECH

the HEDGE @rule11tech

HISTORY OF networking
THE PAST IS PRELUDE

questions