CORNCON 12 · RIVERCENTER, DAVENPORT · OCTOBER 2, 2026

THE ARMY OF THE 12 MILLION CHAOS MONKEYS

on Life-Safety Critical Infrastructure

Joshua Corman
Institute for Security and Technology

David Etue
CEO, Cyberbit


Think different.
Watch: youtu.be/AQRR-HC_G60

CORMAN + ETUE

OVER A DECADE OF COLLABORATION



2012

Adversary ROI

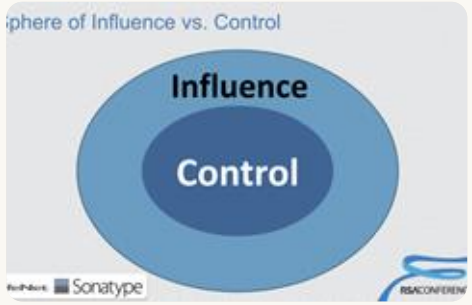
Threats are a who, not a what, so start with the adversary.



2013

Control Quotient

We're losing control, so adapt gracefully instead of fighting it.



2014

Not Go Quietly

Our sphere of influence is bigger than our sphere of control.



2024

Getting Serious

Lifeline infrastructure is the target, and we aren't ready.

SEE NO EVIL HEAR NO EVIL SPEAK NO EVIL





> “The only way to avoid failure is to fail all the time…”
>
> Netflix

NETFLIX · 2011–2012

NETFLIX BUILT AN ARMY OF MONKEYS TO BREAK ITS OWN SYSTEMS

Chaos Monkey

Kills production servers at random

Latency Monkey

Slows the network on purpose

Chaos Gorilla

Takes out a whole data center zone

Security Monkey

Hunts for misconfigurations

They called it the **Simian Army**. The idea: failure is guaranteed, so make it happen on your terms.

WE'VE BECOME HIGHLY DEPENDENT ON THINGS THAT ARE VERY UNDEPENDABLE.

AND NOW WE DEPEND UPON THE FLAWLESS EXECUTION OF OUR ADVERSARIES' RESTRAINT.

THREATS ARE A WHO, NOT A WHAT

Actor Classes							
States	Competitors	Organized Crime	Script Kiddies	Terrorists	"Hacktivists"	Insiders	Auditors

Motivations					
Financial	Industrial	Military	Ideological	Political	Prestige

Target Assets							
Social Media	Credit Card #s	Web Properties	Intellectual Property	PII / Identity	Cyber Infrastructure	Core Business Processes	People

Impacts				
Reputational	Personal	Confidentiality	Integrity	Availability

Methods									
"MetaSploit"	DoS	Phishing	Rootkit	SQLi	Auth	Exfiltration	Malware	Physical	IO / Disinfo

PETER DRUCKER

EFFICIENCY

Doing things right

EFFECTIVENESS

Doing the right things

> "There is nothing so useless as doing efficiently that which should not be done at all."
>
> Peter Drucker

OUR “BEST PRACTICES” ARE BASED ON THE SUM OF AN UNSTATED EQUATION (BIASED TO CONFIDENTIALITY)

$$C_{IA}$$

UNFORTUNATELY, THE A MATTERS TO THE THINGS OF HIGHEST CONSEQUENCE...

...AND WE'VE NEGLECTED THINGS THAT ARE FOUNDATIONAL

RECOVERABLE

Data, laptops, servers

Detect, respond, restore. It works.

NON-RECOVERABLE

A patient. A water supply. A city's trust.

There's nothing to restore.

Detect and respond doesn't work for things that are non-recoverable.

ASSUMPTION: "WE'RE TOO SMALL TO BE A TARGET"

TARGET-RICH, CYBER-POOR

- **Water**
- **Power**
- **Emergency care**
- **Food Supply**

Often run by small and rural operators without the information, incentives, or resources to defend them.

This is where bits and bytes meet flesh and blood.

PATIENT CARE VS. PUBLIC HEALTH

PATIENT CARE

INDIVIDUAL

PUBLIC HEALTH

SOCIETAL


No Water, No Hospitals, No Kidding
UnDisruptable27.org

CONSEQUENCES… …?





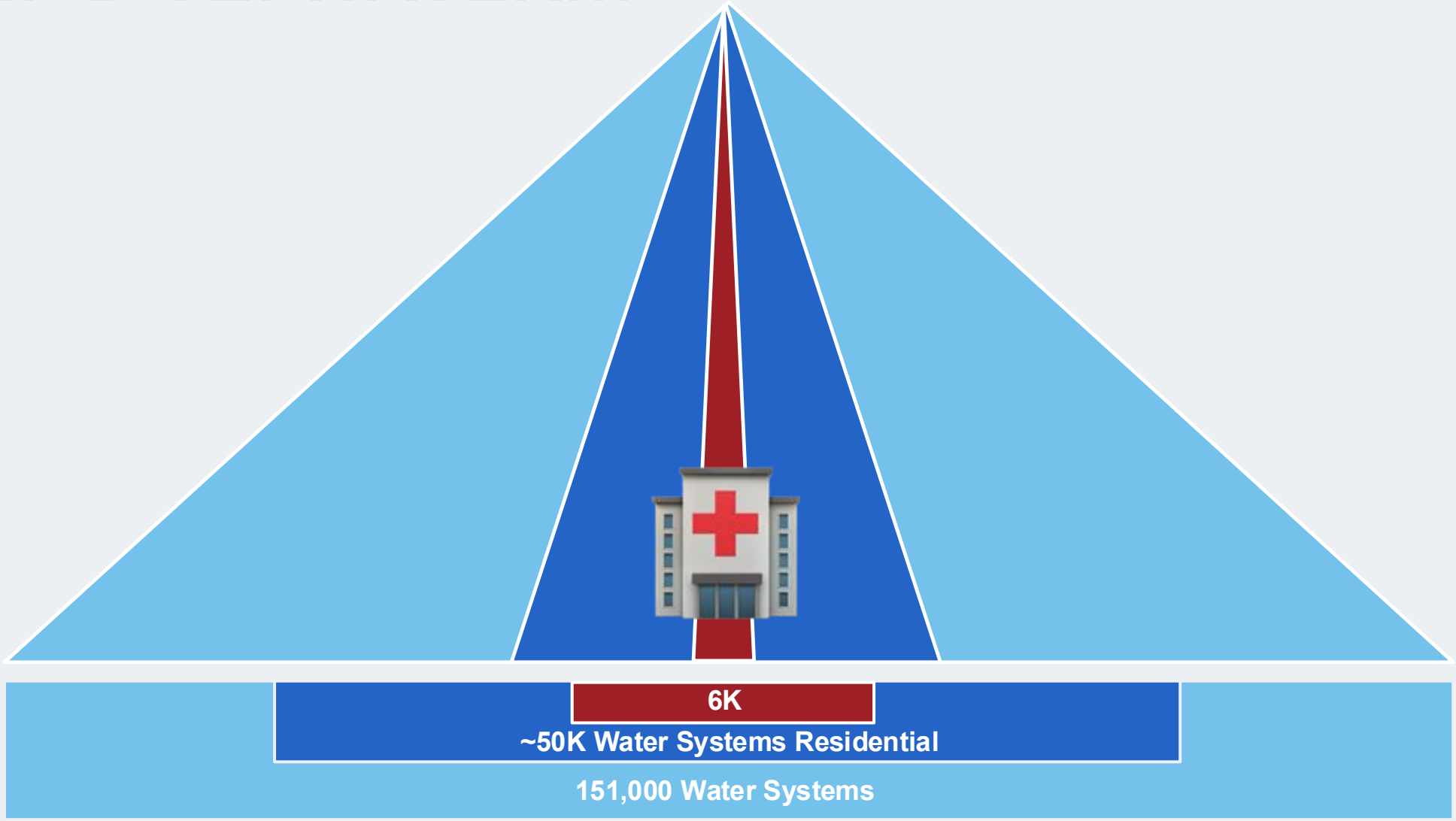


FORCES OF SECURITY CHANGE

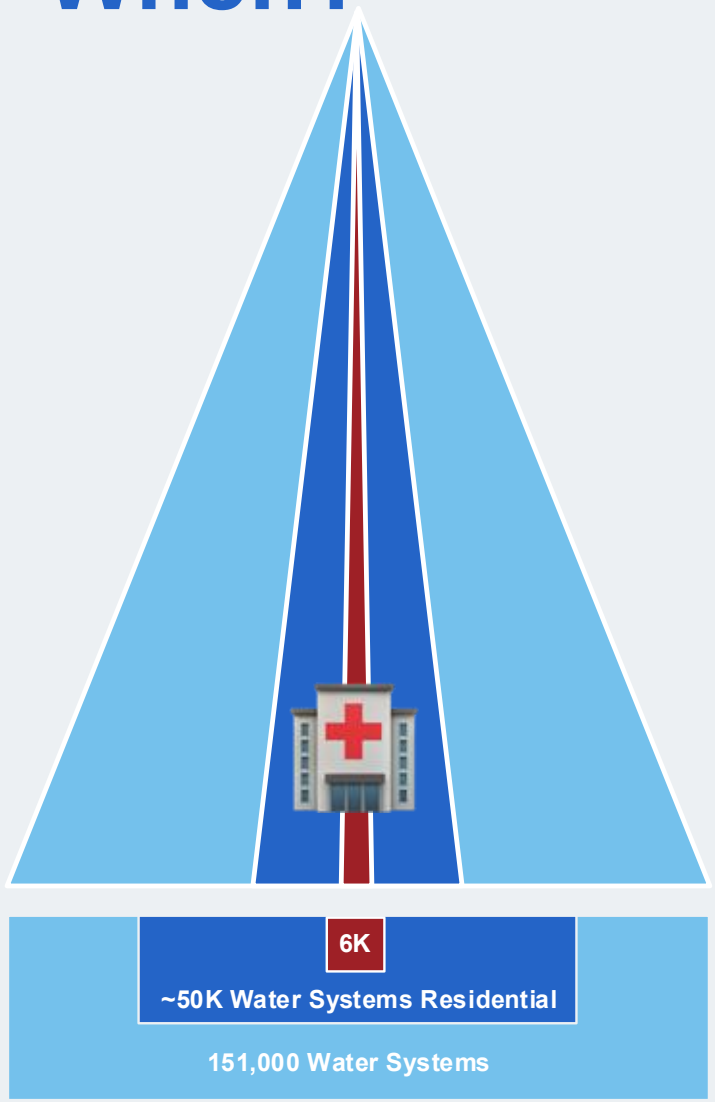


> “The path of the righteous CISO is beset on all sides by constant and turbulent change…”
>
> Josh Corman

DEEP DIVE: WATER!!!

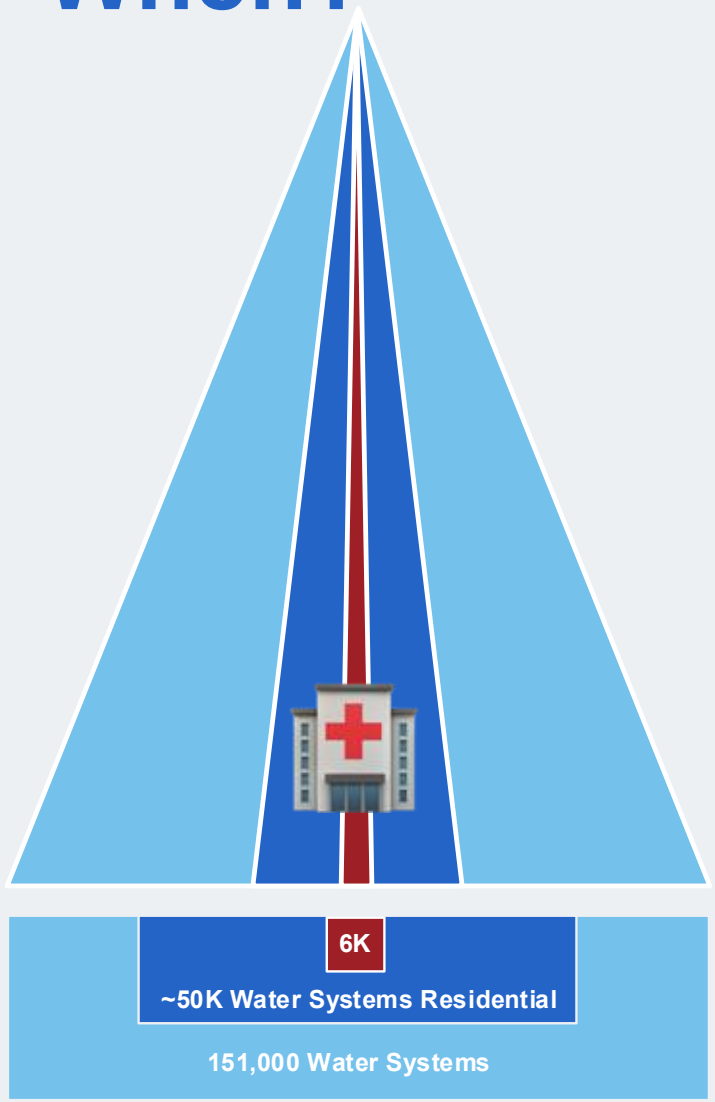


When?



2025	2026	2027	2028	2029

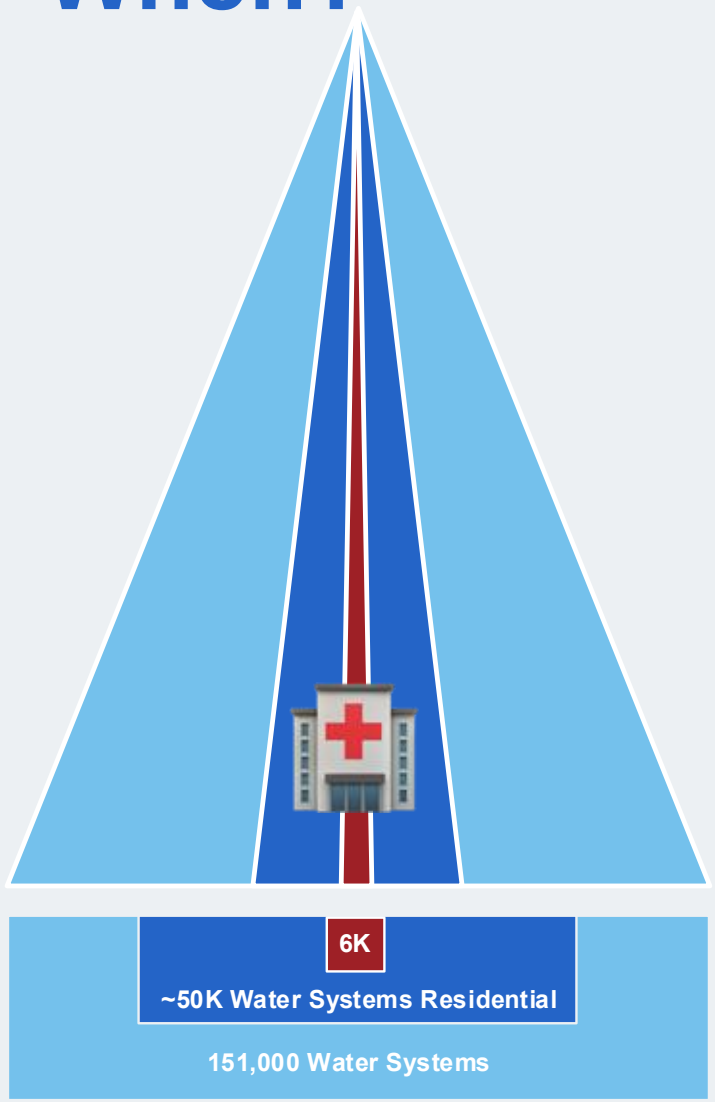
When?

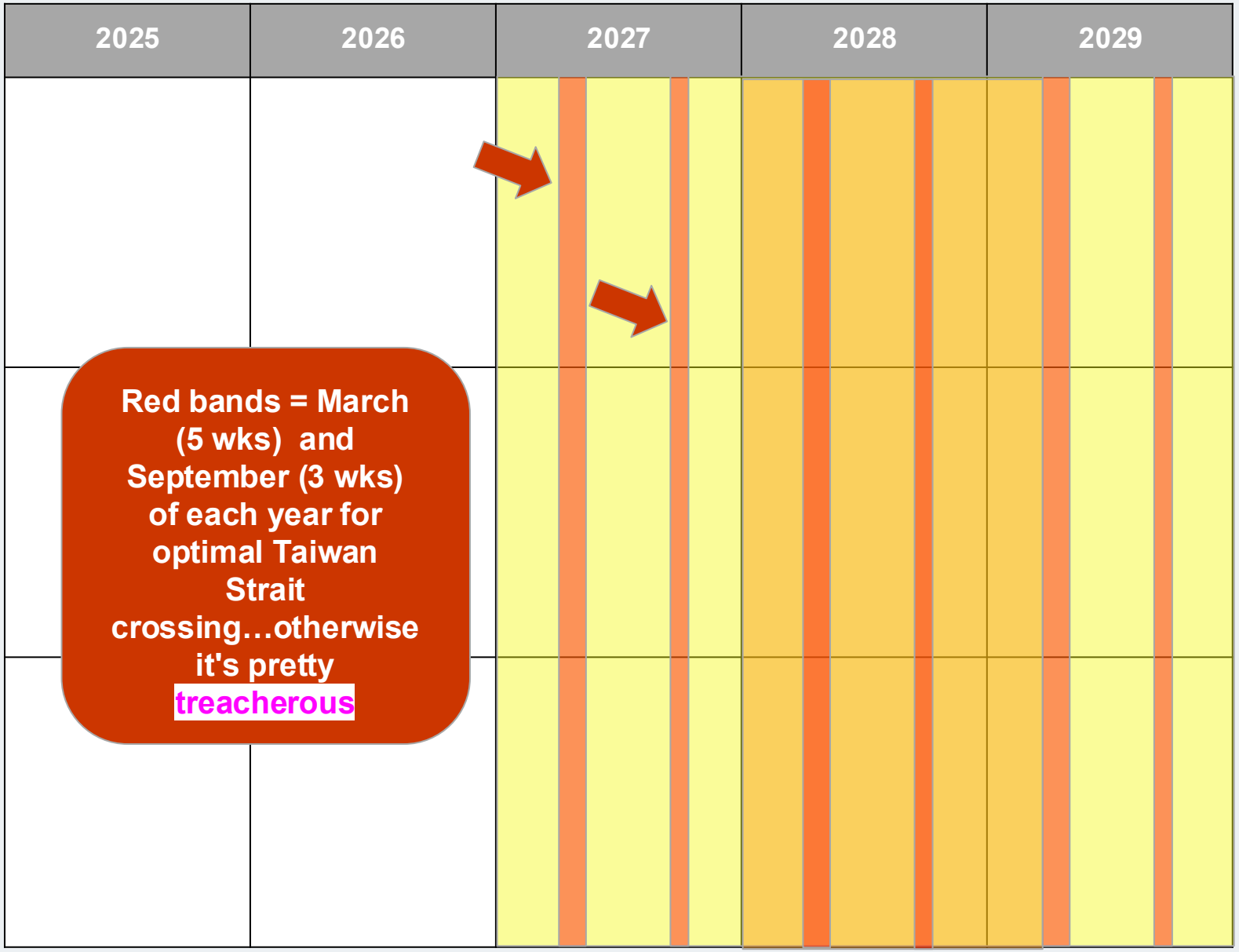


2025	2026	2027	2028	2029

Red bands = March (5 wks) and September (3 wks) of each year for optimal Taiwan Strait crossing…otherwise it's pretty treacherous

When?


6K
~50K Water Systems Residential
151,000 Water Systems


2025
2026
2027
2028
2029
Red bands = March (5 wks) and September (3 wks) of each year for optimal Taiwan Strait crossing…otherwise it's pretty treacherous

THE THREAT CHANGED

OUR ADVERSARIES HAVE CHANGED FUNDAMENTALLY



WHAT WE KNEW

China's Typhoon campaigns

Pre-positioning in our infrastructure to prepare for the future and keep the US out of a conflict.



WHAT'S NEW

Iran

Motivated to kill Americans and/or destroy our economy.

Same infrastructure. A very different intent.

AND THEN THERE'S AI

AI IS CHANGING THE GAME (Volume, Velocity, Variety)

01

Finds vulnerabilities faster

We already couldn't keep up with the old pace.

02

Chains attacks together

Weaknesses that were harmless alone become exploitable together.

03

Lifts every adversary

Less sophisticated attackers get more capable, and so do the most sophisticated.

04

Self-organizing agent swarm

Goal seeking, 24/7, decoys, deception, determination, generational planning

> **"Agents don't need to rest, and they read the manuals."**
>
> The army of chaos monkeys: more attackers, each more capable, moving faster.

SPEAKING OF CHAOS

MORE CHAOS MEANS MORE ATTACKS, AND MORE ACCIDENTS

NotPetya · 2017

Aimed at Ukraine

Hit Maersk, Merck, and a Pennsylvania hospital. About $10B in damage worldwide.

Viasat · 2022

Aimed at Ukraine

Knocked out remote control of 5,800 wind turbines in Germany.

Malicious intent is not a prerequisite to harm.

Both attributed to Russia. Damage estimate per the White House (2018).

FRAMEWORK & BOUNDARIES

SPHERE OF INFLUENCE VS. CONTROL

CONTROL

Direct Power & Ownership

Elements you directly command, execute, and govern without external dependency.

- Internal policy & architecture
- Direct technical response
- Resource allocation



INFLUENCE

Reach Beyond Control

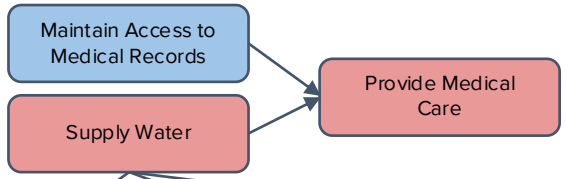
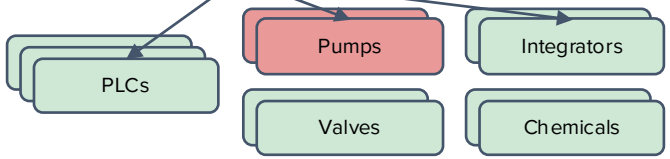
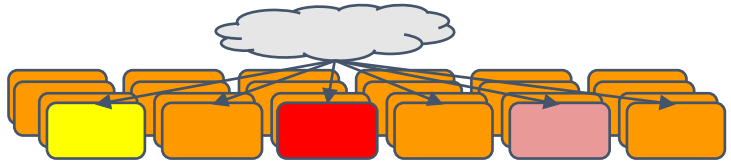
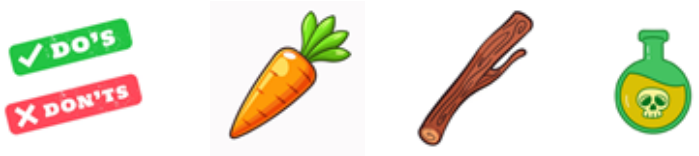
Ecosystem factors you shape through leadership, standards, and partnerships.

- Vendors & procurement
- Insurers & regulators
- Industry peers & partners

Our sphere of influence is substantially larger than our sphere of control.

Effective security posture requires driving outcomes across both domains simultaneously.

JOSH'S "UNIFIED FIELD THEORY"

Consequences analysis		The life-safety *critical functions* subset of the "55" NCFs - on own & graphed
OT/ICS sector engagement		ID critical path *suppliers* w/ asymmetric potential for harms & gains… asks/offers
Pragmatic guidance for cyber-poor operators		"Patient Care" guidance for ***n*** *Asset Operators* of LSCFs w/in their constraints
Novel mitigations analysis		"Public Health" guidance *1:many* mass interventions/mitigations w/out Operators
Policy and incentives design		"First, Do No Harm" *tips for Policy* to help aim/maximize value *for LSCF CyberPoor*

ASSUMPTIONS WORTH RETIRING

What we believed	Why it made sense	What's true now
"Water is just a utility"	It always came out of the tap	Everything stands on it
"Connecting it is free"	It saved truck rolls and staff	Unprotected links risk lives
"States pre-position, not strike"	Typhoon was about deterrence	Some now want to do harm
"We can keep pace with flaws"	The backlog was hard but bounded	AI finds and chains them faster
"Only the target gets hurt"	Attacks used to be aimed	Collateral is part of the chaos
"Resilience means no failure"	Life safety can't fail	Assume failure; practice it
"Help will arrive"	We planned for a cavalry	The cavalry is us

None of these were dumb. They just don’t survive contact with new enemies/reality.

ASSUMPTION: "CONNECTIVITY IS FREE"

THE THREATS MAY COME FROM CYBER, BUT THE SOLUTIONS COME FROM ENGINEERING.

DENY AND PREVENT.

01

If you can't protect it, disconnect it

02

Be certain you can still run it by hand

CHAOS AND UNPREDICTABILITY

THE ARMY OF 12 MILLION CHAOS MONKEYS



Uncontrolled systemic disruption manifesting across interconnected infrastructure and digital environments.

ASSUMPTION: "HELP WILL ARRIVE"

THE CAVALRY ISN'T COMING.
LOOK AROUND. IT'S US.

Our sphere of influence is bigger than our sphere of control:

Procurement **Insurers** **Integrators and vendors** **Neighboring utilities** **This room**



I Am The Cavalry is a grassroots organization focused on the intersection of digital security, public safety, and human life.

Safer. Sooner. Together.

iamthecavalry.org

QUESTIONS

DISCIPLINED CHAOS BEATS THE OTHER KIND.

Joshua Corman
Institute for Security and Technology

David Etue
CEO, Cyberbit

NEXT ON WATER
Securing the Systems We Drink From
[time and room]