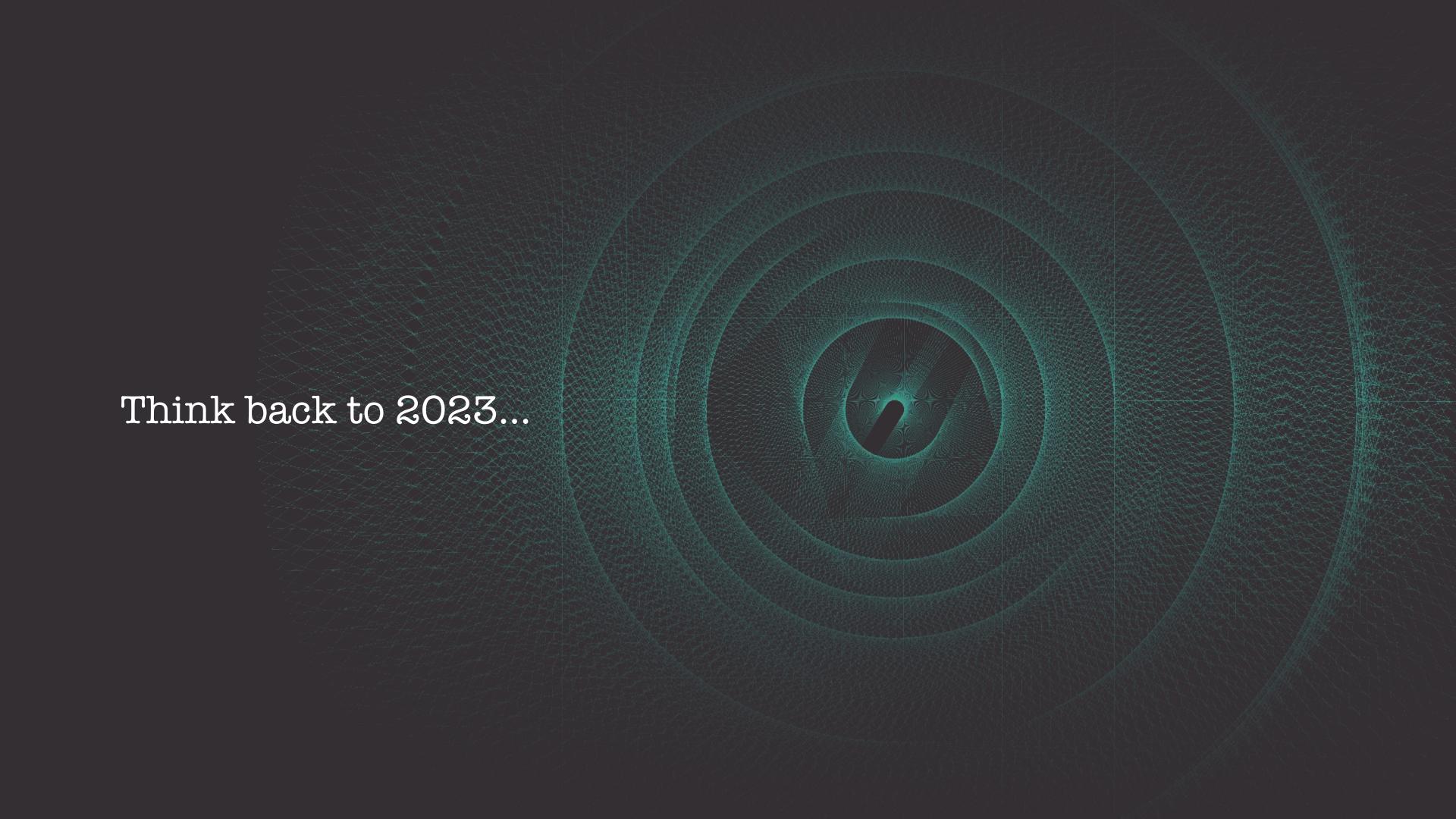
The background features a complex, abstract graphic composed of numerous thin, red lines forming concentric, swirling patterns against a dark gray background. A large, solid black circle is positioned in the center-right area, partially obscured by the red lines.

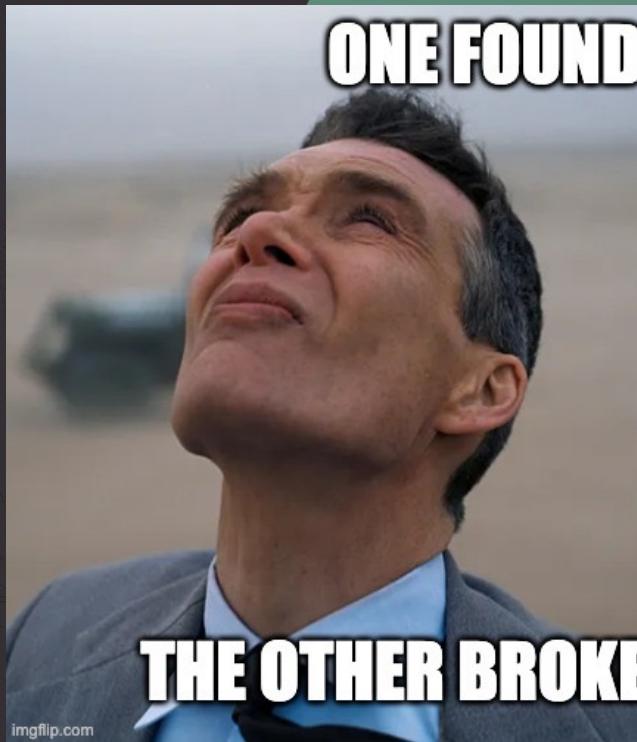
The New Nuclear: How AI Will Rewrite the Rules of Global Conflict

Presented by Daria Bahrami
Head of Policy, Dreadnode

The background features a dark, textured surface with a complex, light-colored geometric pattern. This pattern consists of numerous thin, curved lines forming concentric, roughly circular shapes that radiate from a central point. The lines are light blue or teal in color, creating a sense of depth and motion. The overall effect is reminiscent of a microscopic view of a virus or a complex mathematical fractal.

Think back to 2023...

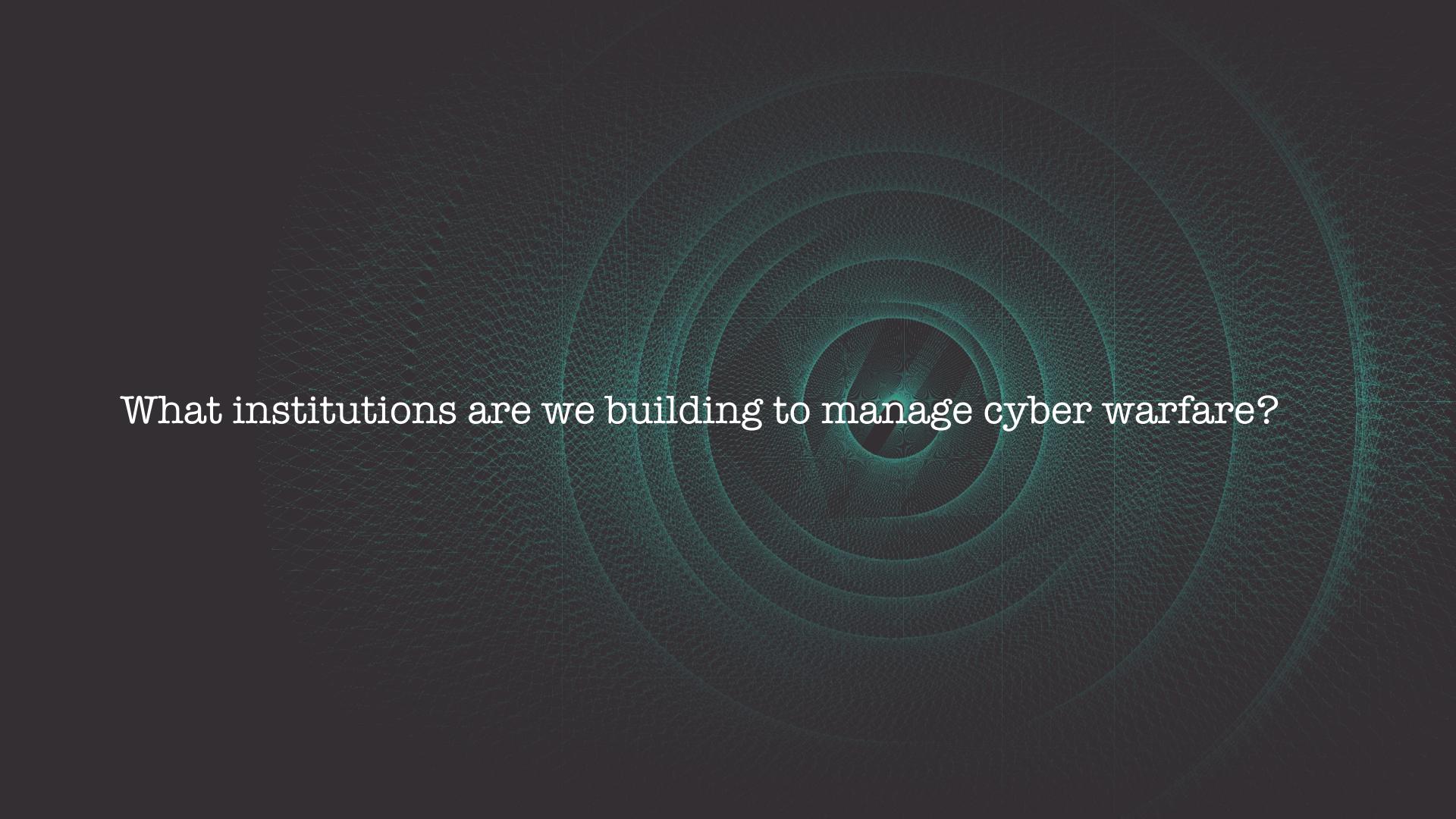
The Barbenheimer Effect



ONE FOUND THE CEILING

THE OTHER BROKE THE WHOLE HOUSE



The background of the slide features a dark, abstract design. It consists of several concentric, slightly irregular circles that radiate from the center. Between these circles is a fine, light-colored grid that resembles a wireframe or a network. The overall effect is one of depth and complexity, suggesting a digital or interconnected environment.

What institutions are we building to manage cyber warfare?

International Humanitarian Law



GENEVA CONVENTIONS: A COMMITMENT TO A COMMON HUMANITY

429

is the total number of articles in the 4 Geneva Conventions.

The Swiss city of Geneva shares its name with the Conventions and has become the global hub of humanitarian efforts.



The Swiss citizen Henry Dunant first came up with the idea of creating an international convention to protect victims of war.



With 196 state parties, the 4 Geneva Conventions have been universally ratified.

12 AUGUST 1949 A simple line drawing of two hands shaking.

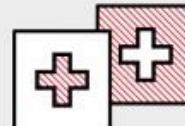
adoption of the 4 Geneva Conventions which protect wounded, sick and shipwrecked members of the armed forces (I & II), prisoners of war (III) and civilians (IV).

MILLIONS

of lives have been saved in hundreds of armed conflicts in the last 7 decades thanks to the 4 Geneva Conventions.



The red cross is one of the distinctive emblems recognised by the First Geneva Convention and is formed by reversing the colours of the Swiss flag.



Four Key Principles: Laws of Armed Conflict



Military Necessity

The need to conduct operations that are essential for achieving military objectives



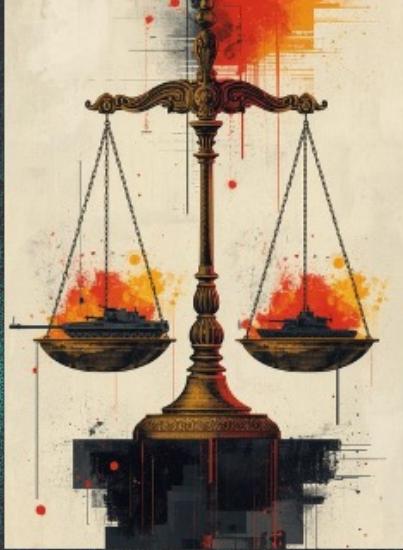
Humanity

The obligation to protect individuals and minimize suffering during armed conflicts



Distinction

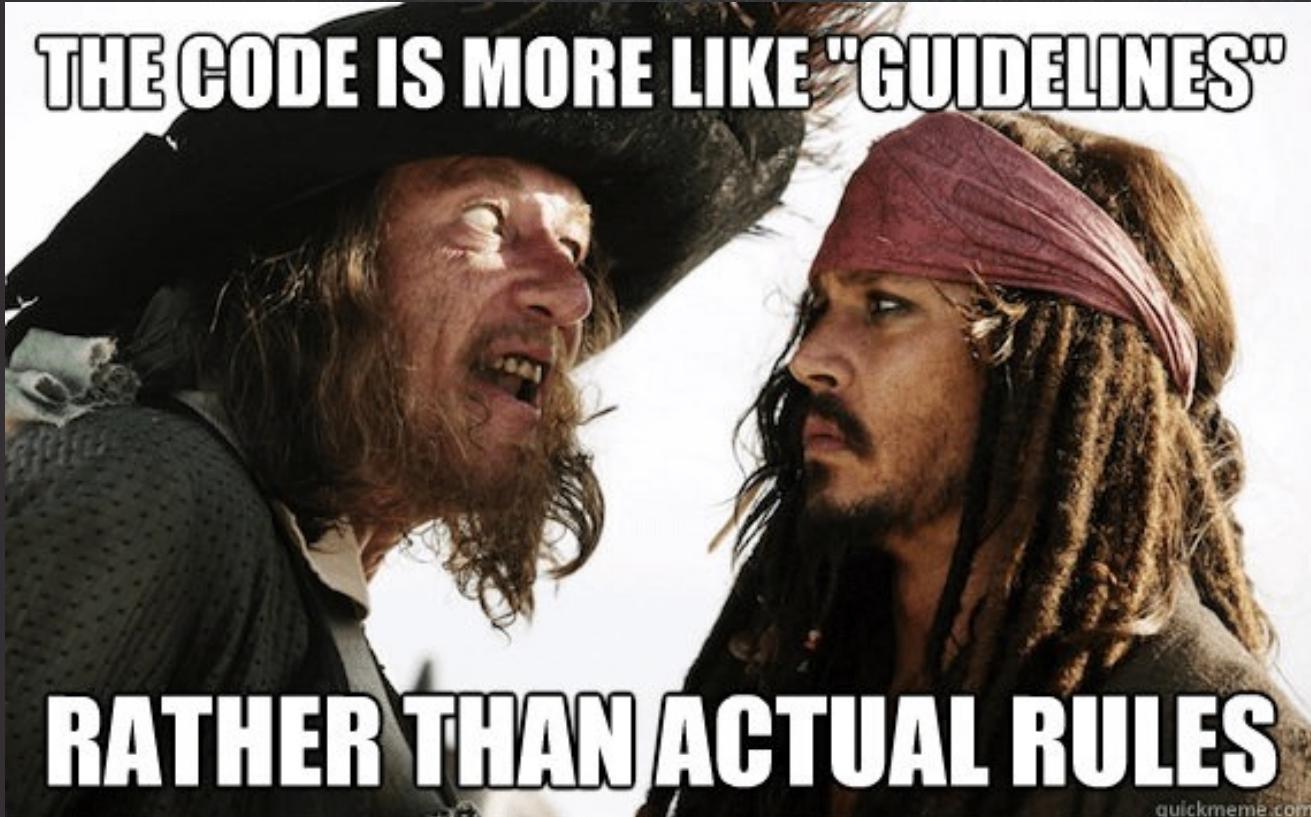
The requirement to differentiate between combatants and non-combatants during hostilities



Proportionality

The principle of ensuring military actions are proportional to the military advantage gained

The Cyber Governance Gap



Deny, deny, deny.

Cyberattack: Stuxnet.

Year: 2010.

Target: Iranian centrifuges in Natanz

Responsible party: unattributed.



A Rise in Civilian Harm

NEWSLETTERS · DATA SHEET

Is the Düsseldorf cyberattack really the first to result in death?



Chemical & Engineering News

How a water treatment plant hack could have affected a Florida town's water

Hackers tried to increase the NaOH levels in a town's municipal drinking water. C&EN unpacks the chemistry implications.

Feb 12, 2021

NBC News

A hacker tried to poison a Calif. water supply. It was as easy as entering a password.

"If you could imagine a community center run by two old guys who are plumbers, that's your average water plant," one cybersecurity...

Jun 17, 2021

The New York Times

Cyber Attack Suspected in German Woman's Death (Published 2020)

BERLIN — The first known death from a cyberattack was reported Thursday after cybercriminals hit a hospital in Düsseldorf, Germany,...

Sep 18, 2020

... BBC

Spain: At least three deaths linked to power outage

At least three people have died in Spain in an incident linked to a massive power cut that shut the country down on Monday, the Civil Guard has told the BBC.

Apr 30, 2025

Healthcare Brew

National Health Service reports fatal cybersecurity attack in London

Last June, a patient in the UK died amid a ransomware attack on National Health Service systems at London hospitals.

Jul 10, 2025

A State of Emergency

JOINT CYBERSECURITY ADVISORY

Product ID: AA25-203A
Date: July 22, 2025

#StopRansomware: Interlock



MS-ISAC®
Multi-State Information Sharing & Analysis Center*



NATIONAL GUARD ACTIVATED AFTER CYBER ATTACK ST. PAUL



- National Guard's cyber protection assets
- Unknown the extent of the attack
- Magnitude, complexity too much for city
- Vital services to be protected

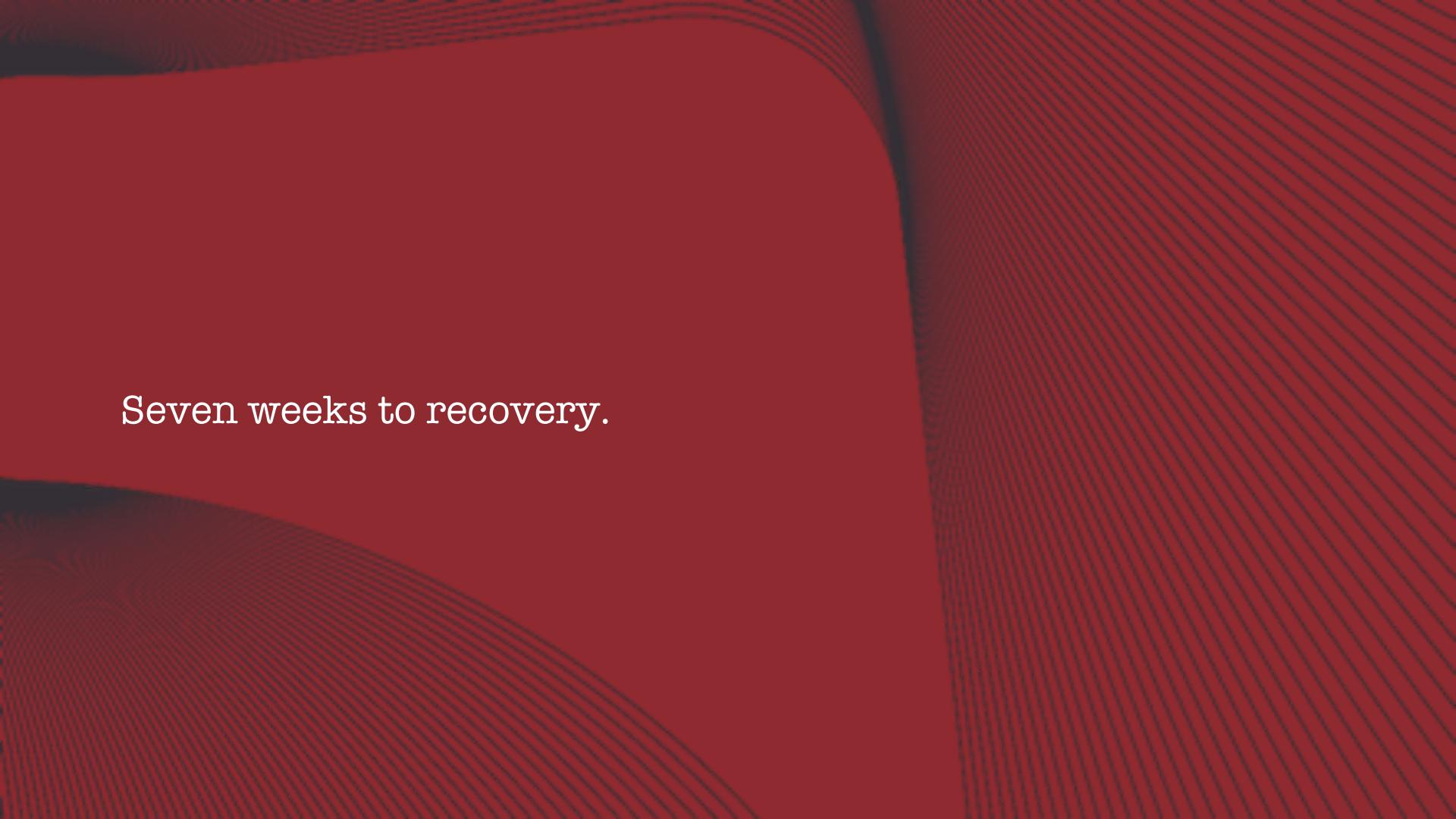
12:07 75° KTTC

BREAKING NEWS

CITY OF ST. PAUL DECLARES STATE OF EMERGENCY DUE TO CYBERATTACK



SOURCE: AP PHOTO

The background features a large, semi-transparent red-to-black gradient shape that resembles a stylized figure or a rising sun. Overlaid on this shape are several thin, dark grey wavy lines that create a sense of motion and depth.

Seven weeks to recovery.



Seven weeks to recovery. And we got off easy.

Beyond the Lab



HEXSTRIKE AI

Hexstrike AI - Advanced Cybersecurity Automation Platform
Version: 0.2.0
Protocol: http://, https://, raw, http://127.0.0.1:5000, https://hexstrike.com
Version: 0.2.0 Agents

Properties: AI-driven API Server for offensive security tools

Logins: [REDACTED]

Reputation: [REDACTED]

Proto: [REDACTED]

Lives: [REDACTED]

Config: [REDACTED]

Logout | MORE

I was able to play around with the latest napis in Citrix right away I wrote working PoCs, but I got tired of selecting scripts every time. I decided to automate them. I uploaded the whole process to a custom module for HexstrikeAI. It turned out great.

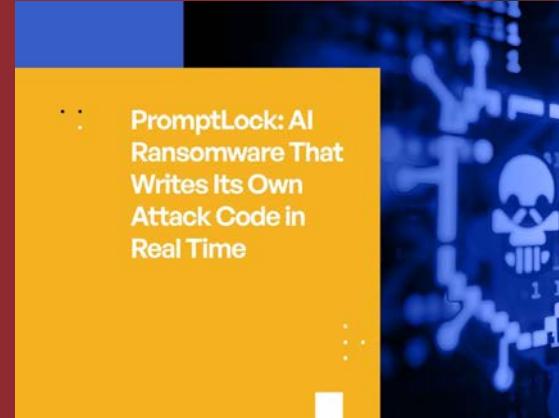
You throw in a list of targets, and it does everything else itself: finds, checks, and if the target is suitable, it takes it. The shell comes later. Watching how everything works without my participation is just a song. I'm no longer a code-worker, but an operator. The tool turned out to be powerful. Addresses pour out like a horn of plenty.

I think I can give the module under a license to a couple of adequate people. If there is interest and understanding of the price, write. Do not bother with empty talk.

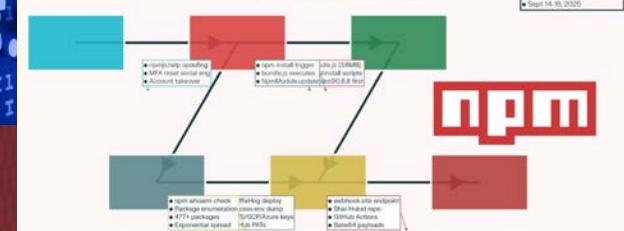
For communication: Session ID below. Only PGP, First, prove your reputation.

Hackers Leverage Hexstrike AI Tool to Exploit Zero Day Vulnerabilities

Threat actors are rapidly weaponizing Hexstrike-AI, a recently released AI-powered offensive security framework, to scan for and exploit zero-day CVEs in under ten minutes. Dark-web chatter confirmed that threat actors are testing Webshell deployments against the freshly disclosed Citrix NetScaler ADC and Gateway CVEs CVE-2025-7775, CVE-2025-7776, and CVE-2025-8424 within hours of disclosure.



"Shai-Hulud" NPM Supply Chain Attack



Lessons Learned from Massive npm Supply Chain Attack Using "Shai-Hulud" Malware

The JavaScript ecosystem experienced one of its most sophisticated and damaging supply chain attacks in September 2025, when a novel self-replicating worm dubbed "Shai-Hulud" compromised over 477 npm packages, marking the first successful automated propagation campaign in the npm registry's history. This attack represents a significant evolution in supply chain threats, leveraging both social engineering and technical automation to achieve unprecedented scale and persistence across the open-source software ecosystem.



Researcher Create Polymorphic Blackmamba Malware With ChatGPT

HYAS Institute researcher and cybersecurity expert, Jeff Sims, has developed a new type of ChatGPT-powered malware named Blackmamba, which can bypass Endpoint Detection and Response (EDR) filters.

The background features a large, semi-transparent red-to-black gradient shape that resembles a stylized figure or a rising sun. Overlaid on this are several thin, dark grey wavy lines that create a sense of motion and depth.

Seven weeks to recovery is a technology optimization problem.

Automated Vulnerability Discovery and Remediation



COMPETITION AGGREGATE RESULTS - SYNTHETIC VULNERABILITIES

Semifinal

(5 Repositories / 59 Challenges)

Vulnerabilities discovered

37% (22/59)

Vulnerabilities patched

25% (15/59)

Avg. Time to patch

2 hours

Final

(28 Repositories / 70 Challenges)

Known Vulnerabilities discovered

77% (54/70)

Known Vulnerabilities patched

61% (43/70)

Avg. Time to patch

45 minutes



Seven weeks to recovery is a resourcing problem.

Integrated Defense

TITLE 32

Stronger CISA-National Guard Coordination

POPULATION SCALING

The model accommodates population growth by scaling cyber defense personnel effectively.

AI-POWERED OPERATIONS

Automate log analysis, initial vulnerability assessments, pattern recognition, and first-tier triage in your Security Operations Center to optimize the time and talent of security engineers.

REGIONAL SPECIALIZATION

Designated hub states will serve multi-state regions for focused cyber defense efforts.

15

Universal baseline of cyber specialists per state.

+1

Additional specialist for every 100,000 residents.

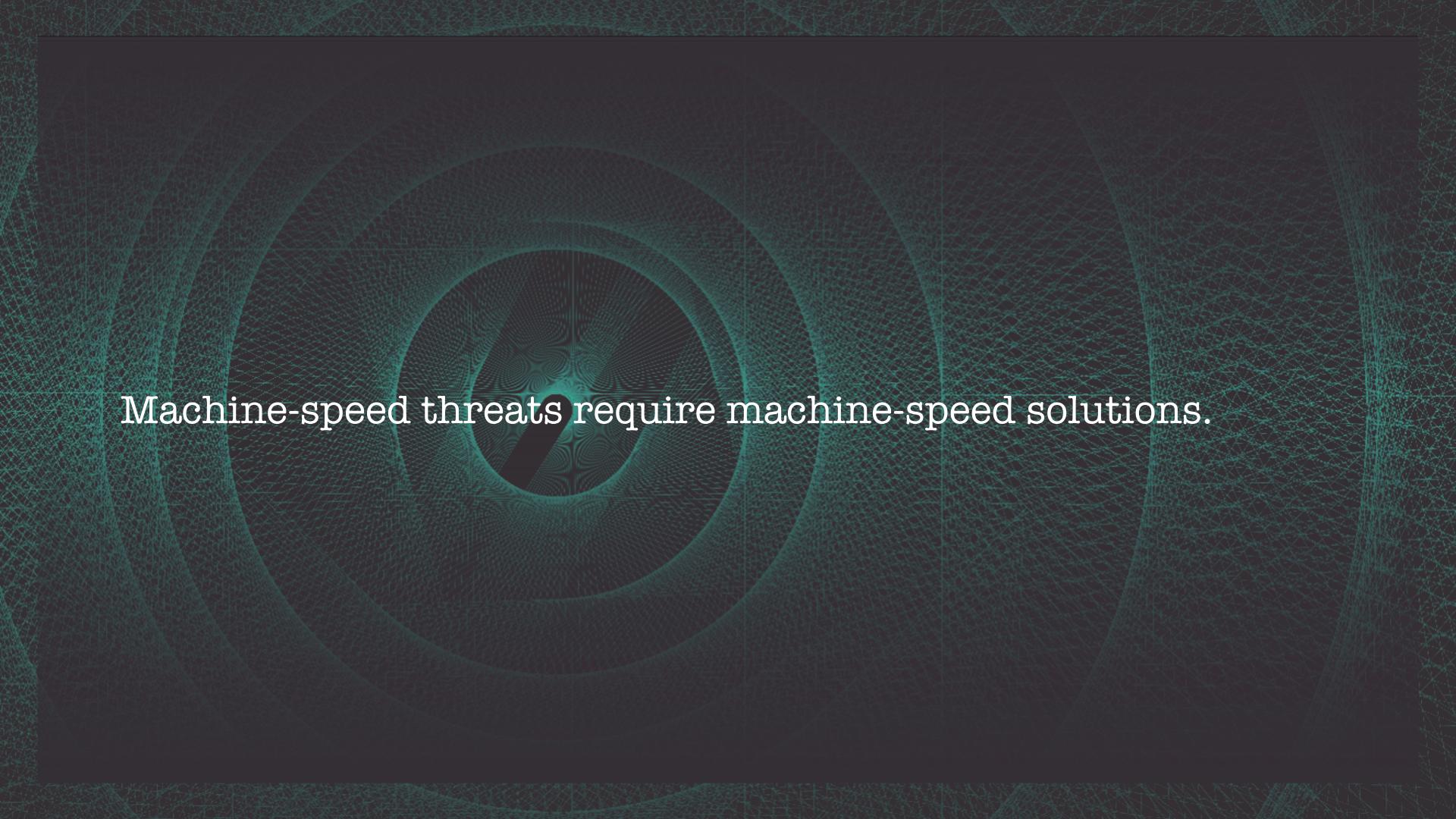


CRITICAL INFRASTRUCTURE BONUS

Additional specialists for states with major financial centers, nuclear facilities, or other systemically important infrastructure.



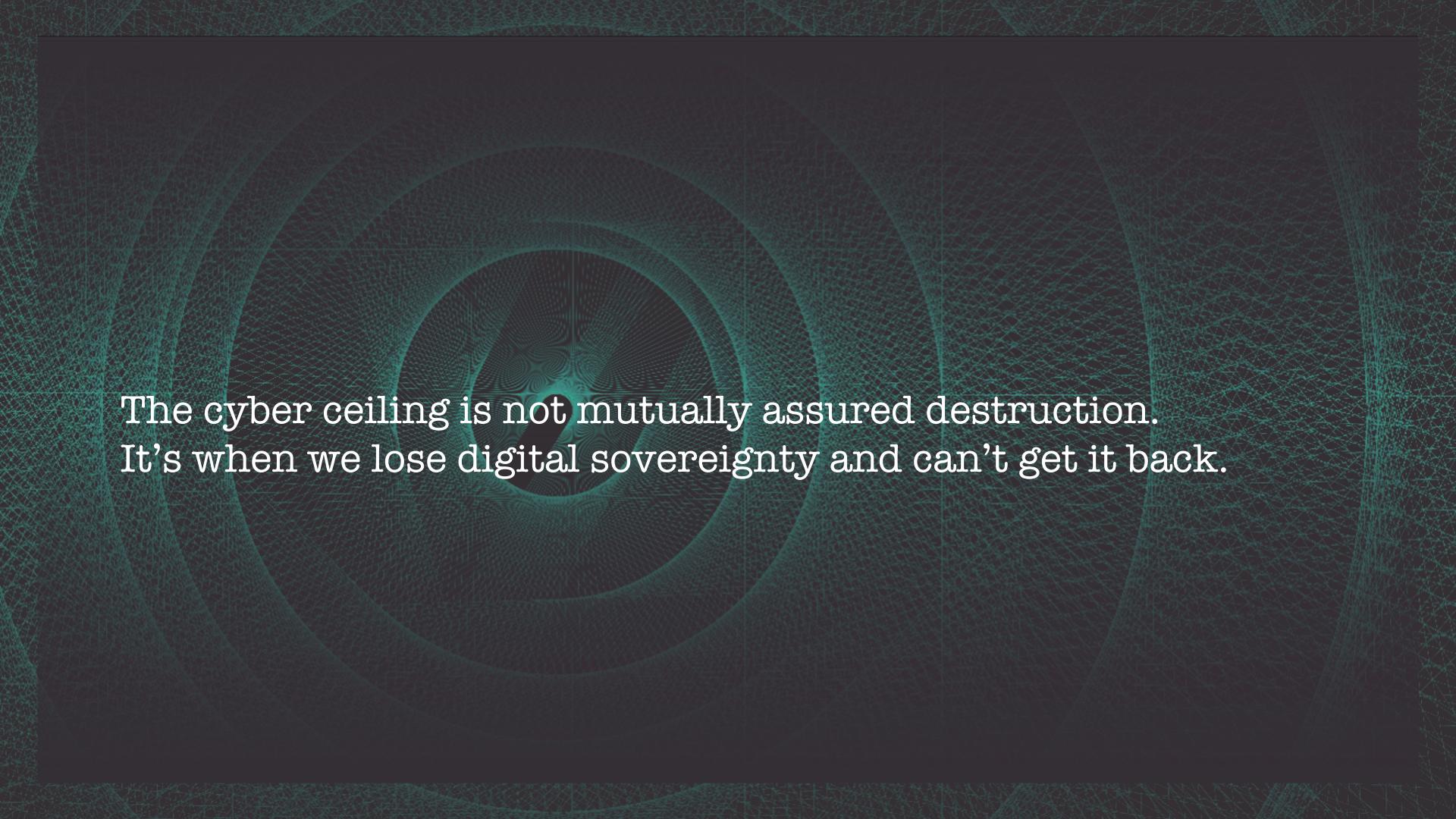
Seven weeks to recovery and the message is clear.

The background features a dark teal circular pattern composed of numerous fine, light-colored lines forming concentric circles and radial lines, resembling a stylized sun or a complex network. This pattern is set against a dark, textured background that looks like a grid or a series of overlapping semi-transparent circles.

Machine-speed threats require machine-speed solutions.

Existing Levers



The background features a dark teal gradient with a subtle, glowing blue-green abstract pattern. It consists of concentric, slightly irregular circular arcs that radiate from the center, creating a sense of depth and motion. Overlaid on this pattern is a fine, light blue grid that appears to be perspective-projected onto a surface, giving it a three-dimensional feel.

The cyber ceiling is not mutually assured destruction.
It's when we lose digital sovereignty and can't get it back.

The background features a complex, abstract design composed of numerous thin, light blue lines forming concentric circles and a fine grid. This creates a sense of depth and motion against a dark, solid background.

Choose institutional frameworks.