
OPERATIONAL
TWILIGHT: APTS,
OT, AND THE
GEOPOLITICS OF
A DYING CLIMATE

WHO AM I?

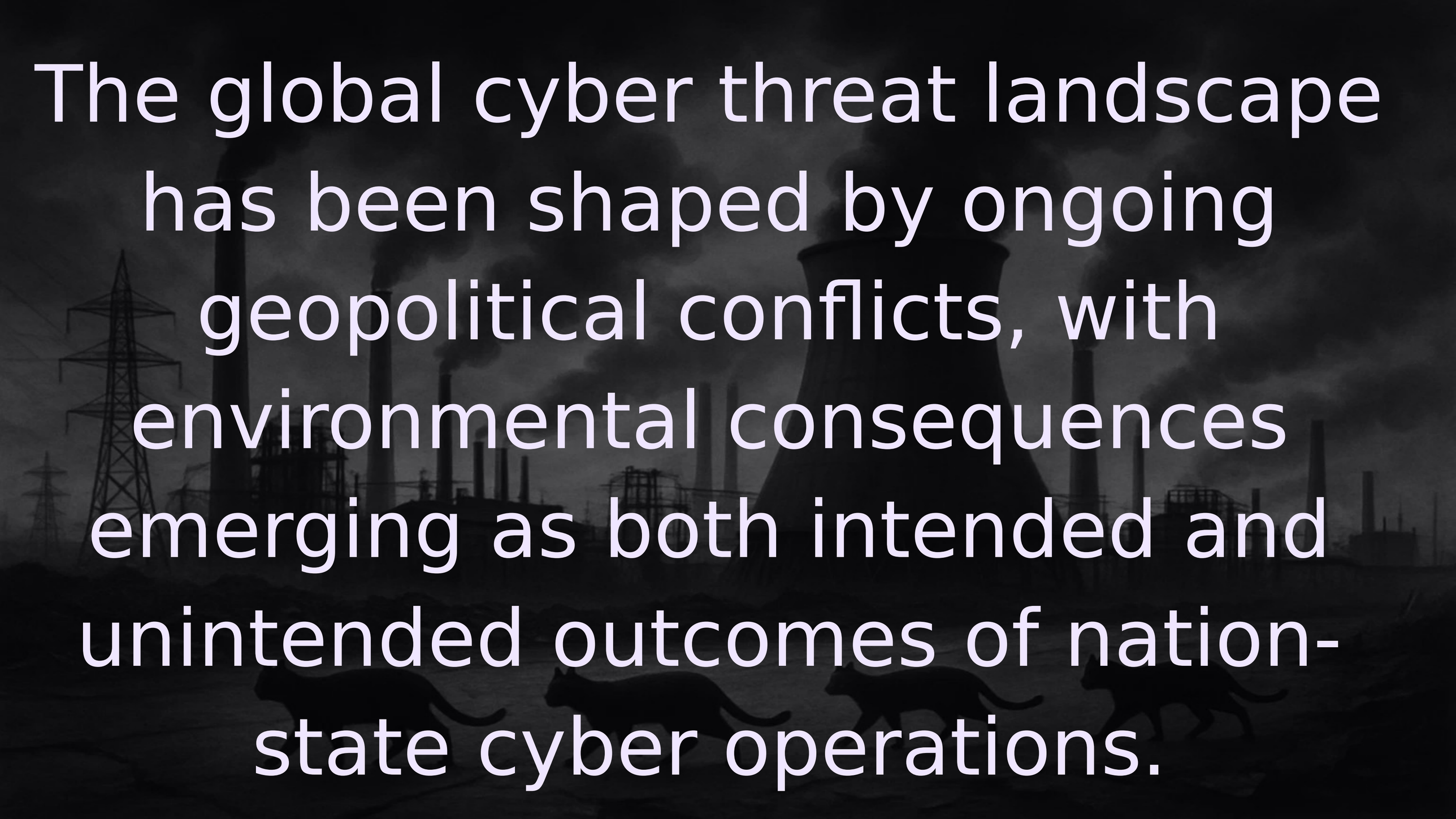
Cybelle is a CTI researcher, Master's student, and co-founder of La Villa Hacker—the first DefCon village for Portuguese and Spanish speakers.

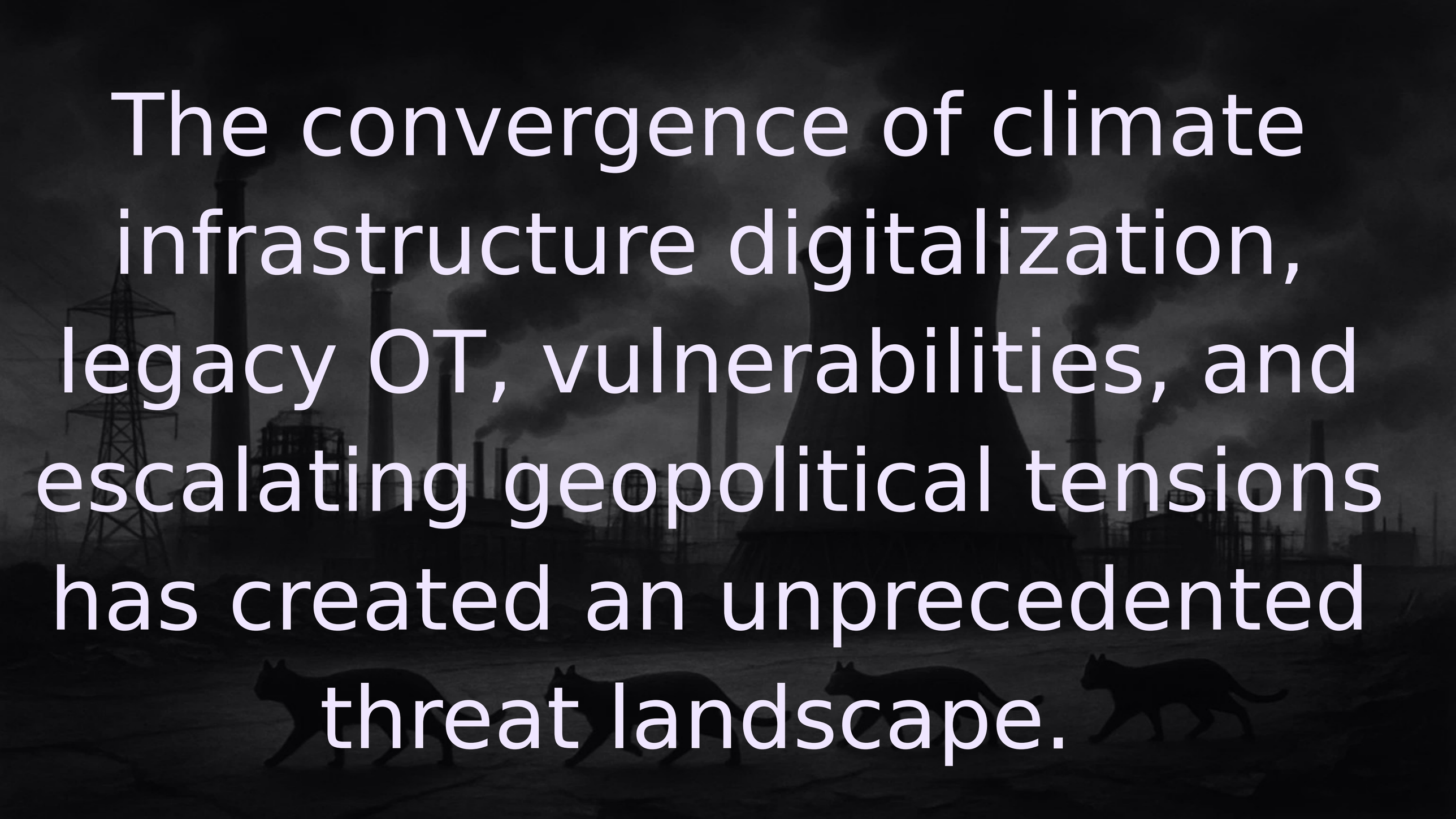
She likes chocolate, tattoos, cats and, travel*

*no necessarily in this order




The State of Climate Cybersecurity in 2025


The global cyber threat landscape has been shaped by ongoing geopolitical conflicts, with environmental consequences emerging as both intended and unintended outcomes of nation-state cyber operations.


The convergence of climate infrastructure digitalization, legacy OT, vulnerabilities, and escalating geopolitical tensions has created an unprecedented threat landscape.

Threat activity surge:

- 340% increase in climate infrastructure targeting (2022-2025)
- 156 confirmed incidents in 2024 (3 per week)
- 89% caused physical damage (people are actually

- + 420 million attacks on critical infrastructure between 2023-2024 (30% increase)
- + 4,800 critical infrastructure organizations reported cyber incidents to FBI in 2024
- $16.6 billion in total cybercrime losses in 2024 (33% increase from

Attack surface growth:

- 50 billion connected environmental devices globally (+400% since 2020)
- 2.3 billion HVAC systems with network connectivity
- 95% of water treatment plants now digitized
- 78% of renewable energy

Attack Surface Comparison

Traditional Enterprise:

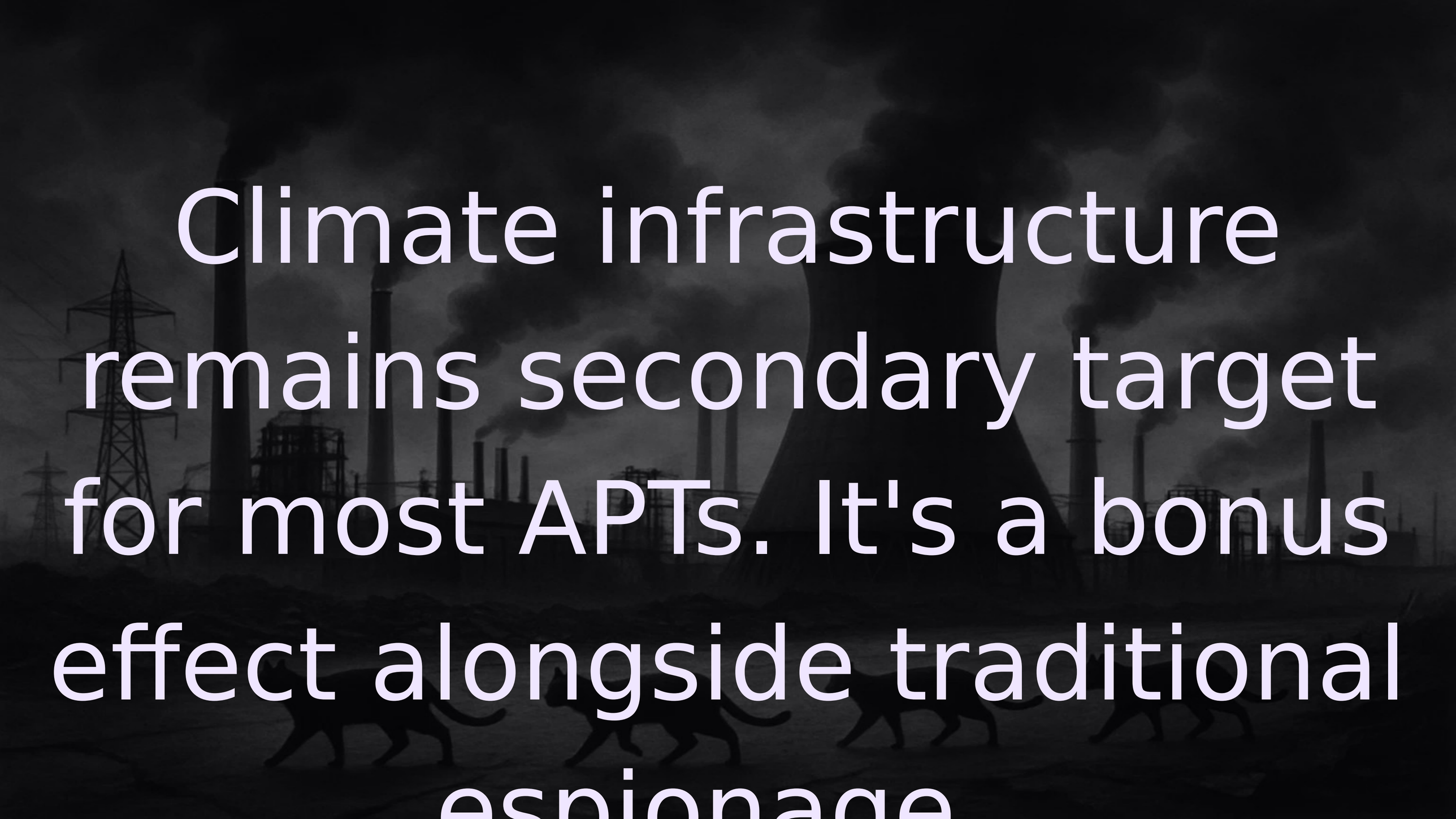
Devices: Workstations, servers, mobile
Protocols: HTTP/S, SMB, RDP, DNS
Impact: Data loss, downtime, financial damage

Climate Infrastructure:

Devices: PLCs, RTUs, smart thermostats, sensors
Protocols: Modbus, BACnet, DNP3, IEC 61850
Impact: Hypothermia, heat stroke


We're applying data center security to thermostat networks


ound Earth's Kill


Climate infrastructure remains secondary target for most APTs. It's a bonus effect alongside traditional espionage

- Attacks are designed to achieve traditional objectives: economic disruption, political destabilization, or military advantage.
- The environmental consequences are overlooked in targeting assessments, they represent significant strategic value to adversaries.

APT climate specialization:

- 12 nation-state APT groups actively targeting climate infrastructure
- 4 nation-states developing environmental warfare doctrine (China, Russia, Iran, North Korea)
- 89% attributed to state-sponsored actors
- 234% increase in climate-themed

How APTs learned environmental warfare

- APTs didn't set out to become environmental terrorists, they stumbled into it.
- Each major industrial attack taught them that physical system manipulation generates exponentially more strategic impact than traditional cyber

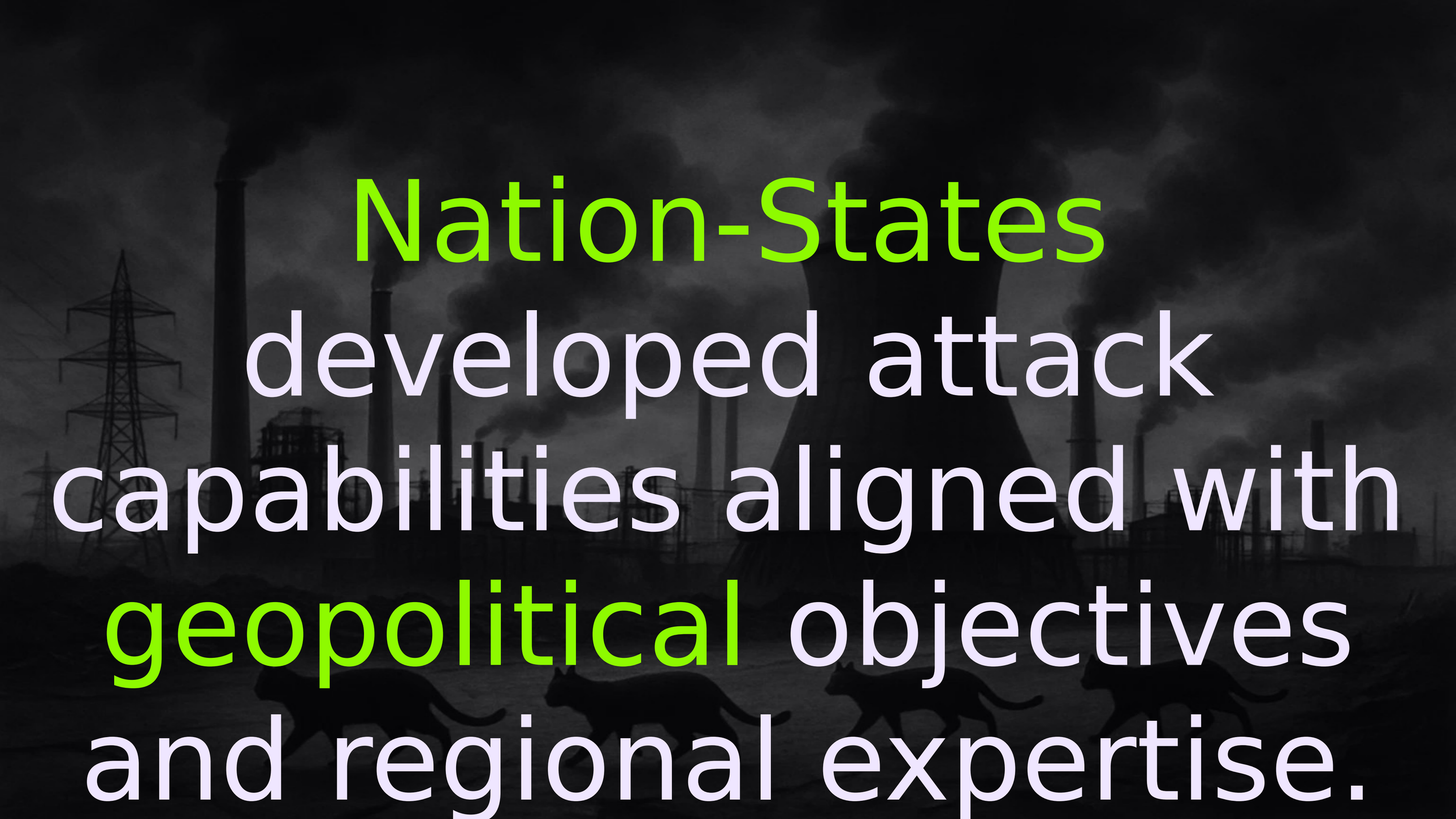
nvironmental cyber warfare tactics

- Timed to maximize impact during stress periods (winter heating, summer cooling, drought conditions, etc.)
- Systems failures creating cascading effects across multiple sectors
- Protocol abuse rather than vulnerability exploitation

Caos, disorder, destabilization. And why not displace populations, hungry, thirsty,

APTs' climate kill pyramid of pain




Nation-States
developed attack
capabilities aligned with
geopolitical objectives
and regional expertise.

INFRASTRUCTURE TARGETING SUMMARY BY SECTOR

SECTOR	CHINA	RUSSIA	IRAN	NORTH KOREA
ENERGY	Water utilities power grids	Power companiess	Oil refineries, power plants	Nuclear facilities
WATER	Future disruption positioning	Active treatment plant	Israeli-tech facilities	Minimal targeting
TRANSPORT	Communications infrastructure	Railway systems	Transportation sector	Defense-relat-only
DEFENSE	Aerospace, manufacturing	NATO entities	Military contractors	Weapons manufacturers

Specialization patterns:

Winter warfare experts
Critical infrastructure + seasonal timing
Pattern: immediate disruption

Water & petrochemicals
Regional destabilization via resource manipulation
Pattern: regional adversary

Technology & agriculture Advanced systems + supply chain attacks
Pattern: long-term

Environmental crime
ESG ransomware + carbon trading theft
Pattern: financial and nuclear intel


Attack
Surface Gone
Green

Climate Infrastructure Threat Surface

Building Automation Systems Devices & Protocol:

- BACnet/IP: 75% of commercial HVAC
- Modbus TCP: Industrial heating controllers

Intelligence Gap: 80% of BAS networks unmapped by defenders

Smart Grid Integration Devices & Protocol:

- AMI Systems: 95M smart meters in US
- Renewable Controls: Solar/wind grid integration

Intelligence Gap: 90% lack grid-climate correlation

Water Treatment Systems Systems Devices & Protocol:

- Chemical Dosing: SCADA-controlled water treatment
- Irrigation Networks: Precision agriculture automation

Intelligence Gap: 95%

Climate infrastructure threats

Every thermostat is now a potential weapon

- Function Code 06: Modbus 'Write Single Register' command
- Changes temperature setpoint: 22°C → 5°C
- Zero authentication required

Your tap water has IP address

- SCADA systems on 192.168.1.100 with default credentials admin/admin
- Modbus TCP water treatment controllers directly internet-facing
- HMI dashboards accessible via port 80 without authentication

Solar panels have more connectivity than most people

- Inverters broadcasting WiFi SSIDs 'SolarEdge_XXXX' with WPS enabled
- Power optimizers responding to unauthenticated SNMP queries

Attack Surface Explosion

Solar Farm

·· 50,000 individually connected inverters

Distributed control, 100% digital

Zero manual operation

Standardized protocols (Modbus, DNP8, IEC 61850)

Water Treatment Plant

200+ PLCs controiling chemical doxing

15 SCADA workstations, Windows 7

24/7 remoote monitoring via VPN

Smart Grid Substation

300 IEDs (intelligent Electronic Devices)

12 protection relays networked

4G/5G primary communications

Wind Farm Operations

120 turbines, each with 20+ sensors

Fiber optic backbone, 99,9% uptime

Prediative maintenance algorithms

Water Treatment Plant

200+ PLCs controlling chemical dosing

15 SCADA workstations, Windows.7

24/7 remote-teolay networkbed

4G/5G primary to 6 control centers

Building Management System

1500 lof sensors per floor

80 VAV controllers networked

Industrial Gas Plant

400 field devices on Ethernet/IP

25 safety instrumented systems

THE RENEWABLE SECURITY PARADOX

ATTACK 30% RENEWABLE CAPACITY DURING PEAK DEMAND

CARBON EMISSIONS SPIKE 300% DURING ATTACK PERIOD

GRID INSTA-BILITY AFFECTS NEIGHBORING REGIONS

FORCES 40% INCREASE IN FOSSIL FUEL ACTIVATION

INTERNATIONAL CLIMATE GOALS DELAYED ~1 MONTH PER ATTACK

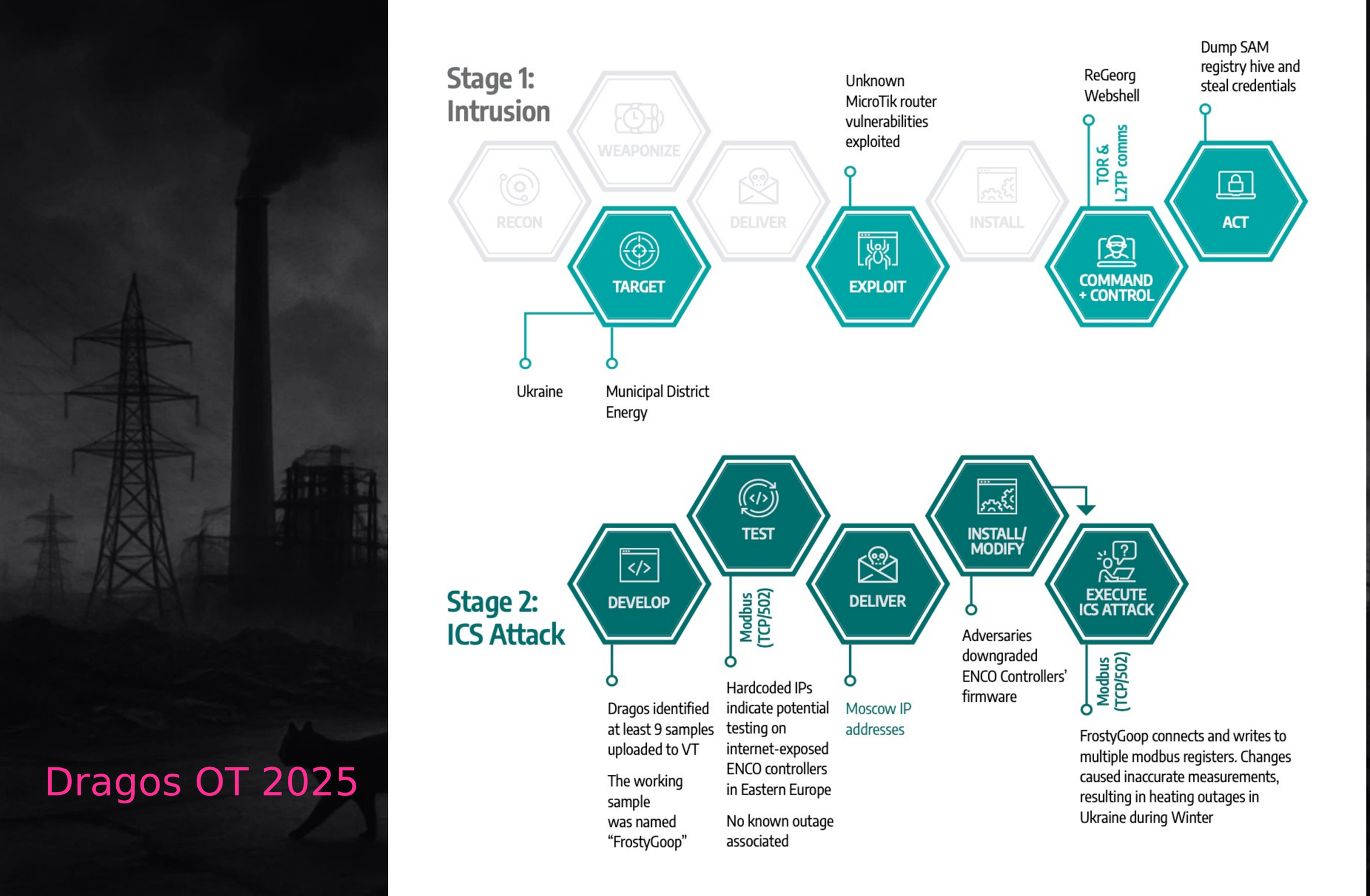

FrostyGoop:
technical
excellence, evil
purpose

January 22, 2024 - Lviv, Ukraine

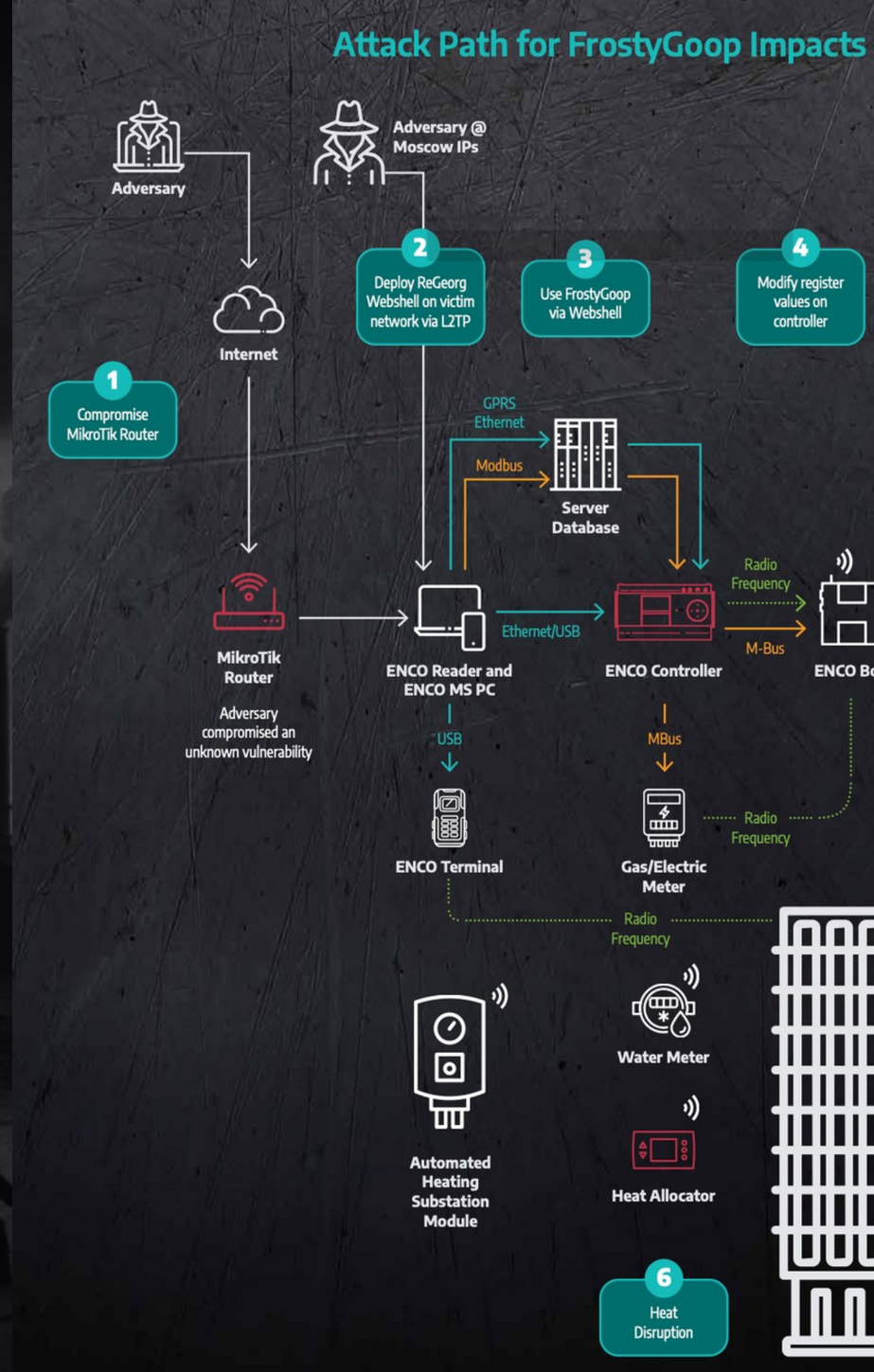
- cyber-attack against a Ukrainian municipal district energy company
- 2-day heating system service
- disruption temperature: -15°C
- 600 buildings without heating
- 30 000 people affected

- The first OT malware to use Modbus TCP and the 9º OT-focused strain reported
- Developed in Go
- Cross-platform compilation: Single executable targets Windows/Linux/ARM industrial controllers simultaneously
- Static linking: no dependencies, self-contained chaos
- Works on air-gapped networks, no missing libraries or interpreters needed

- Concurrent execution: Go routines for multi-target attacks
- Built-in networking: perfect for protocol manipulation ⟶ native TCP stack handles Modbus protocol flawlessly on unreliable industrial networks
- Anti-analysis: Go compiles to optimized machine code with stripped symbols, making the original source code and variable names nearly impossible to recover.



Dragos OT 2025



Dragos OT 2025

The brilliant design attack:



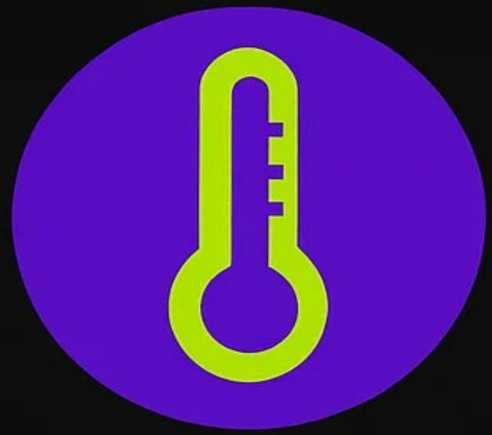
WEATHER CORRELATION

Timed 48–72 hours before extreme cold for maximum impact



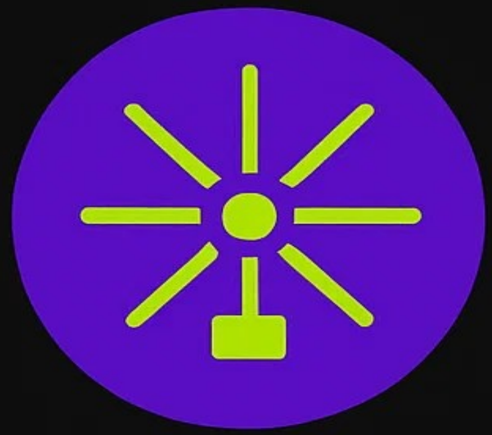
STEGANOGRAPHIC PERFECTION

All commands look like legitimate HVAC maintenance



PHYSICS AS PERSISTENCE

Once heating stops, thermodynamics does the damage



ZERO EXPLOITS NEEDED

Uses legitimate Modbus functions for illegitimate purposes



MINIMAL FOOTPRINT

MINIMAL FOOTPRINT

~200 lines of Go achieve nation-state level impact in <50 KB

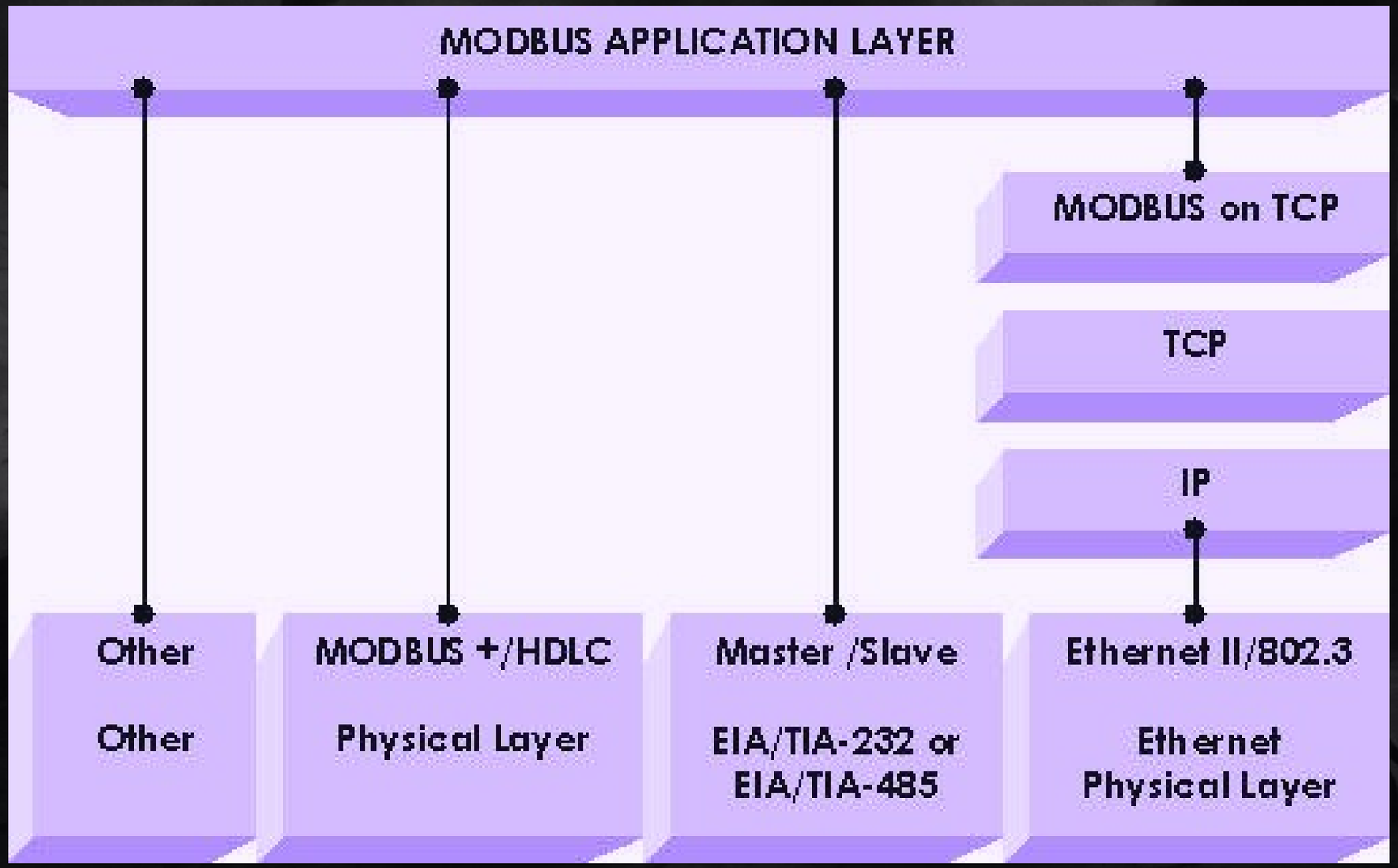
What the hell is Modbus?

- Born in 79 by Modicon (Schneider Electric)
- Industrial communication protocol for PLCs and controllers
- It's the language that thermostats, pumps, and sensors use to talk
- Standard way for computers to send commands like "turn on heating" or "set temperature to 22°C

Technical foundation:

- Local serial communication (controller-device architecture)
- Security model: "Physical access required"
- TCP/IP + internet exposure = 0 security

The Technical Foundation:



- Local serial communication (controller-device architecture)
- Security model: "Physical access required"

Modbus communication Protocol



SCADA/DCS

Gateway



Modbus

Modbus Master



PLC

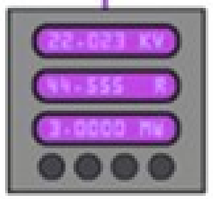
Modbus Slave



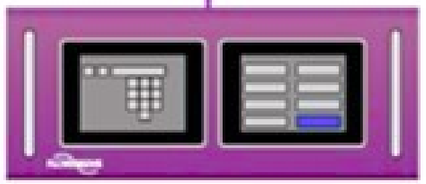
Flow Meter



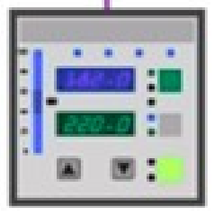
Drives



Power Monitors



Control Actuators



Field Loop Controller

Vintage protocols, modern apocalypse

Zero Authentication - Anyone can connect

No Encryption - Everything in plaintext

No Integrity Checks - Easy to manipulate

What’s the problem?

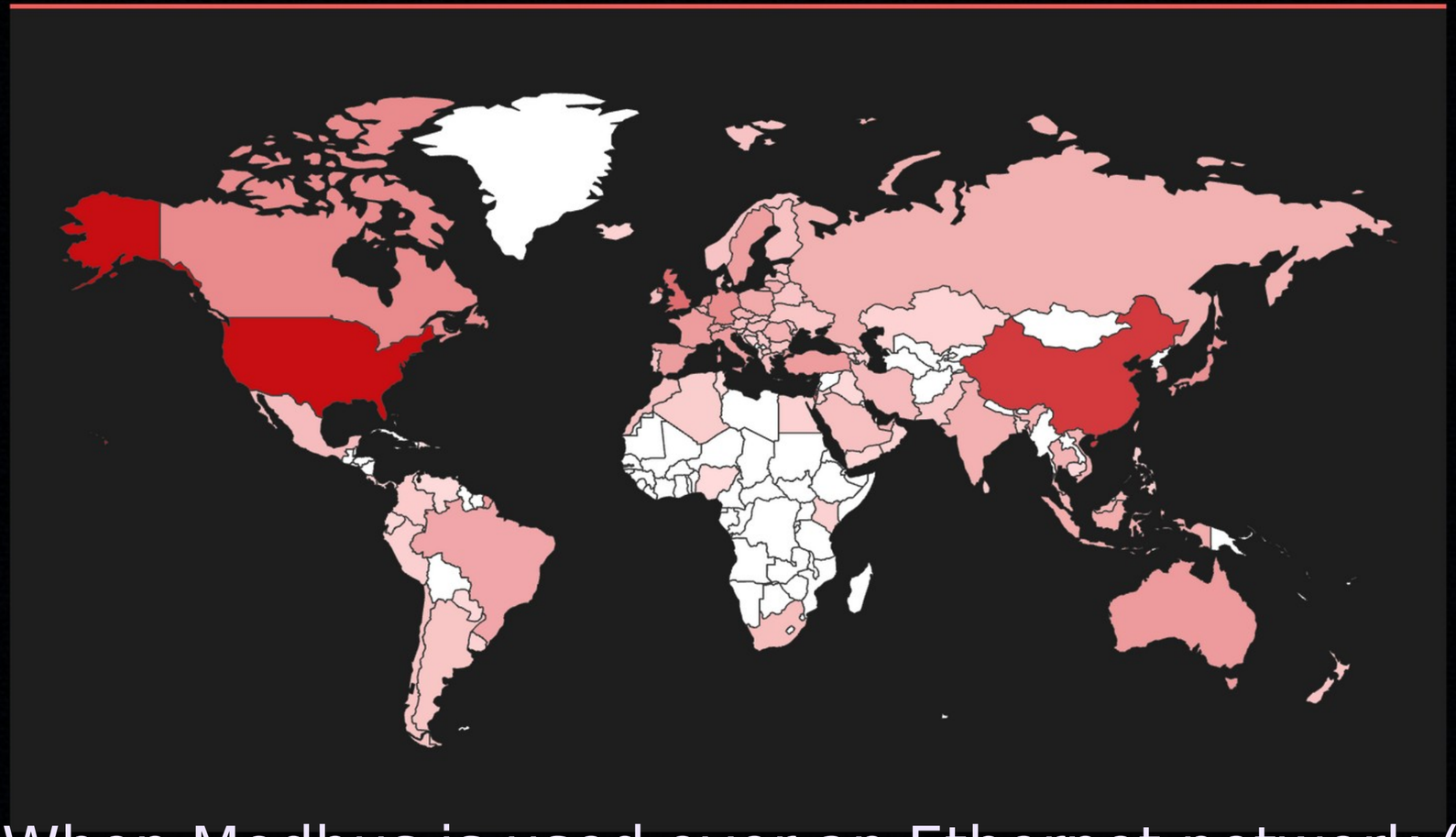
- It's everywhere but fundamentally insecure
- Designed for reliability, not security
- Easy to exploit once you're on the network
- Powers critical infrastructure we depend on daily

Shodan Report

`port:502`

Total: 814,619

// GENERAL



Countries

United States	460,701
China	164,879
United Kingdom	36,407
Israel	29,937
Singapore	15,254

When Modbus is used over an Ethernet network (TCP/IP), it typically utilizes port 502.

SHODAN JUI
12th


CTI for the end
of the world

Critical-Nexus Framework

Layer 1
Climate &
Geopolític Intel

Geopolitical
Analysis
- Regional
tensions
- Economic
sanctions
-Alianças
estratégicas

Climate Analysis
- Extreme
weather events
-Seasonal
vulnerabilities

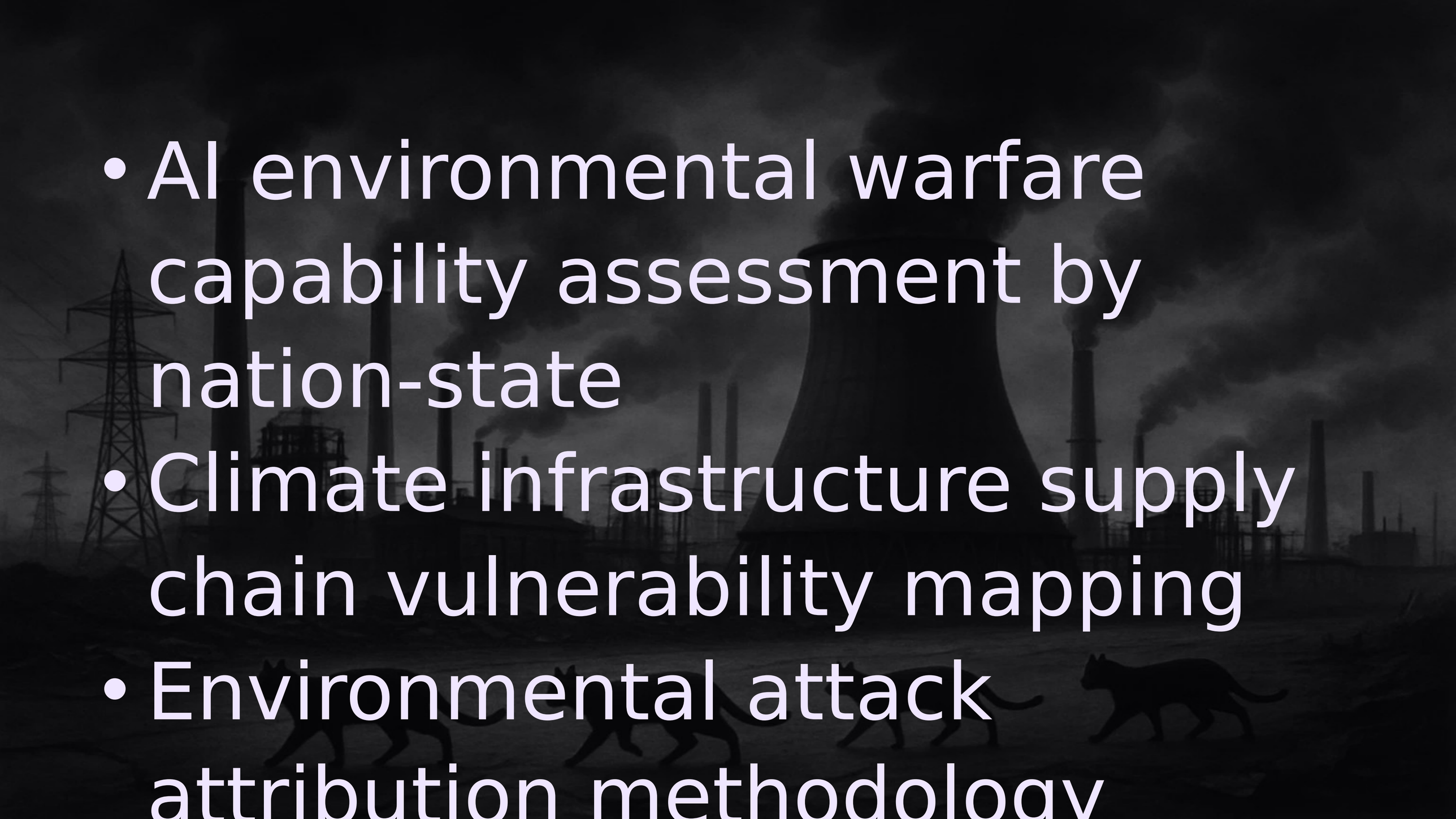
Layer 2
CTI
- APT Tracking
-TTPs
- C2
Infraestructure
- Tools &
exploits
- Hacktivismo
- Active
groups
- Motivations
and ideology
- Technical
capacity
- Organized
crime
-RaaS

Layer 3
OT vuln analysis
- Asset Inventory
- PLCs/RTUs/IEDs
-Industrial
Protocolos
- Firmware
versions
- Vulnerability
Assessment
- OT CVEs
- Insecure configs
- Supply chain
dependencies
- Operational
impact
- Process critical
Criticidade do
processo
- Redundancies

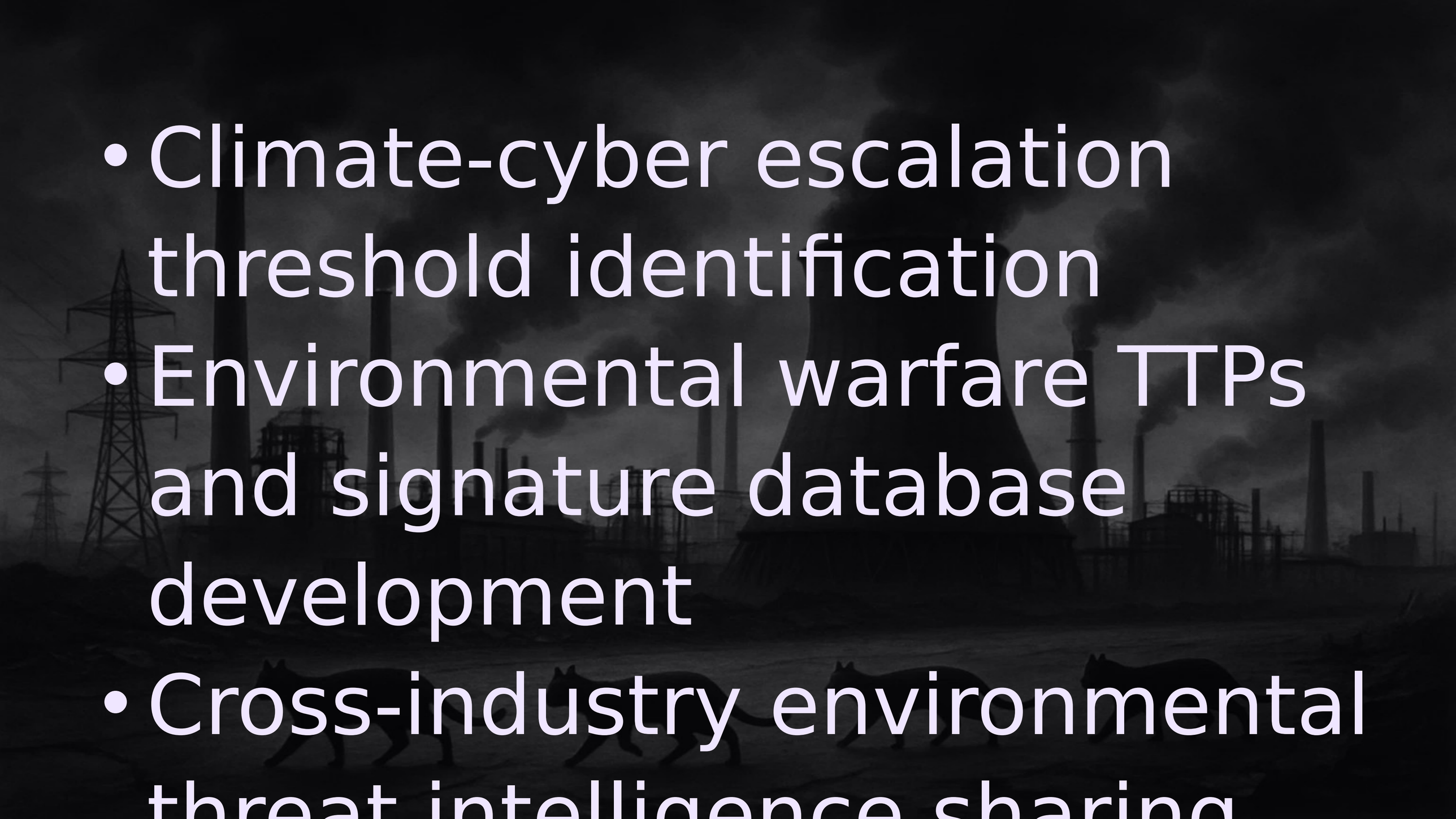
Layer 4
Correlation &
Priorization
- Risk Scoring
Engine
-Probabilidade
(geopolitics ×
adversary capacity)
- Impact
(operational ×
climatic)
- Detectability
- Playbooks
Automatization
-Detection
process
- Contention
- Recovery
-Indicators

AI-Enhanced Environmental Warfare

- Environmental Impact Prediction: 94% accuracy in carbon footprint increase calculations
- Geopolitical response prediction: Diplomatic pressure scoring based on attack characteristics
- Attribution evasion optimization: Attack parameter tuning to avoid



- AI environmental warfare capability assessment by nation-state
- Climate infrastructure supply chain vulnerability mapping
- Environmental attack attribution methodology



- Climate-cyber escalation threshold identification
- Environmental warfare TTPs and signature database development
- Cross-industry environmental threat intelligence sharing

Actionable Intelligence

- Early warning indicators
- Environmental monitoring (48-72 hour weather forecasts)
- Geopolitical intel (diplomatic crisis escalation)
- Technical intel (APT reconnaissance activity spikes)
- Seasonal vulnerability windows

Cross-functional requirements:

- IT Security + OT Security + Facilities Management
- Environmental Safety + Public Health + Emergency Response
- Threat Intelligence + Incident Response + Business Continuity


The Climate
Cyber
Apocalypse

Escalation scenarios

The Global Thermostat War

- Coordinated international HVAC attacks during extreme weather
- 50+ countries affected simultaneously
- Mass climate refugee crisis, potential NATO Article 5 for

The Renewable Energy Collapse

- Systematic supply chain compromise of global clean technology
- Multi-year efficiency degradation campaigns
- Forced return to fossil fuels, energy-dependent

The Water Wars Cascade

- Cyber-amplified water scarcity triggering regional conflicts
- Major river system cyber-physical attacks
- Regional conflicts escalate to

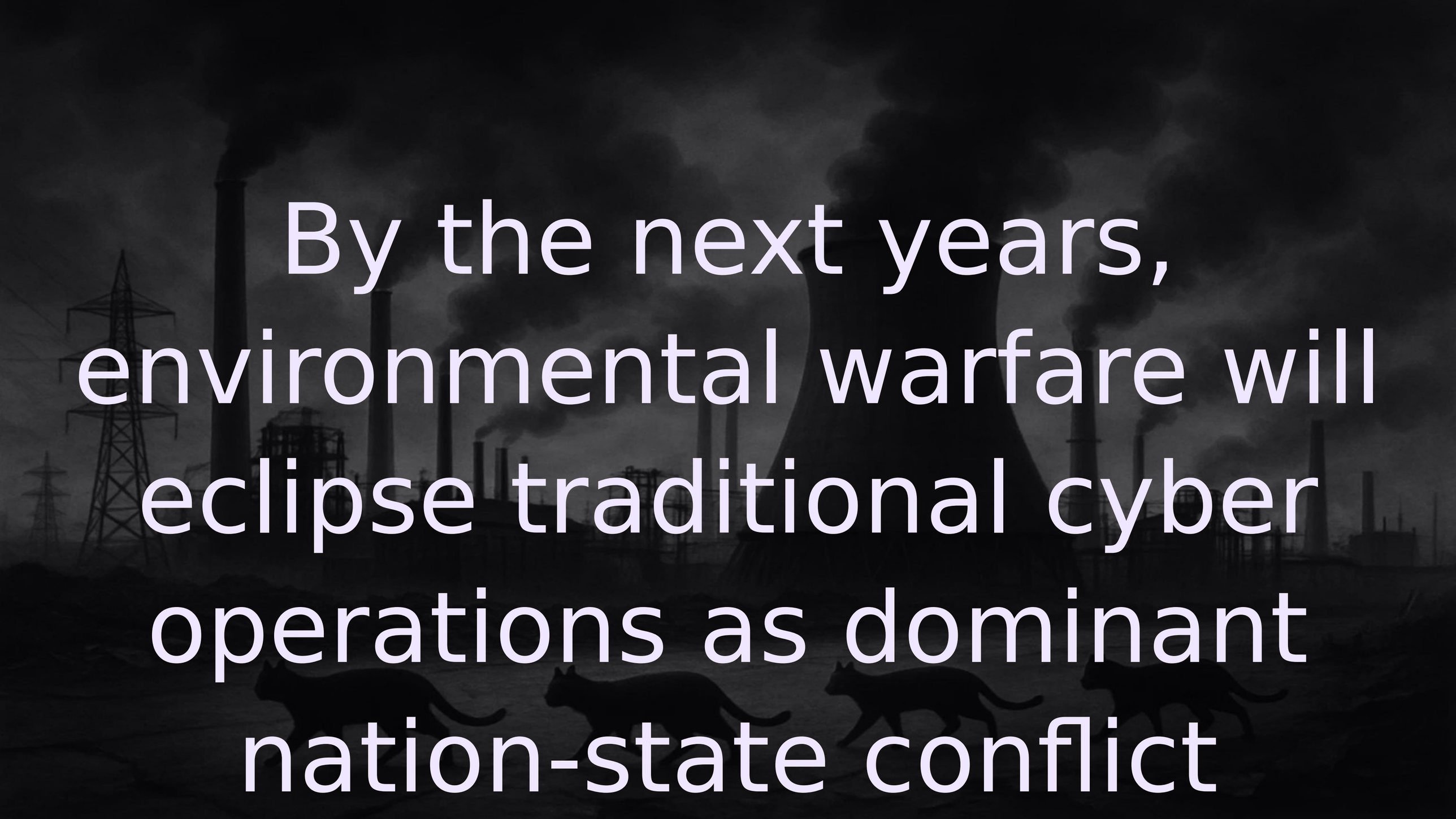
f coordinated attacks with extreme w

- Power grid exploitation during hurricane storm recovery
- Water system compromises during droughts
- HVAC system disruption during extreme temperatures
- Emergency communication system

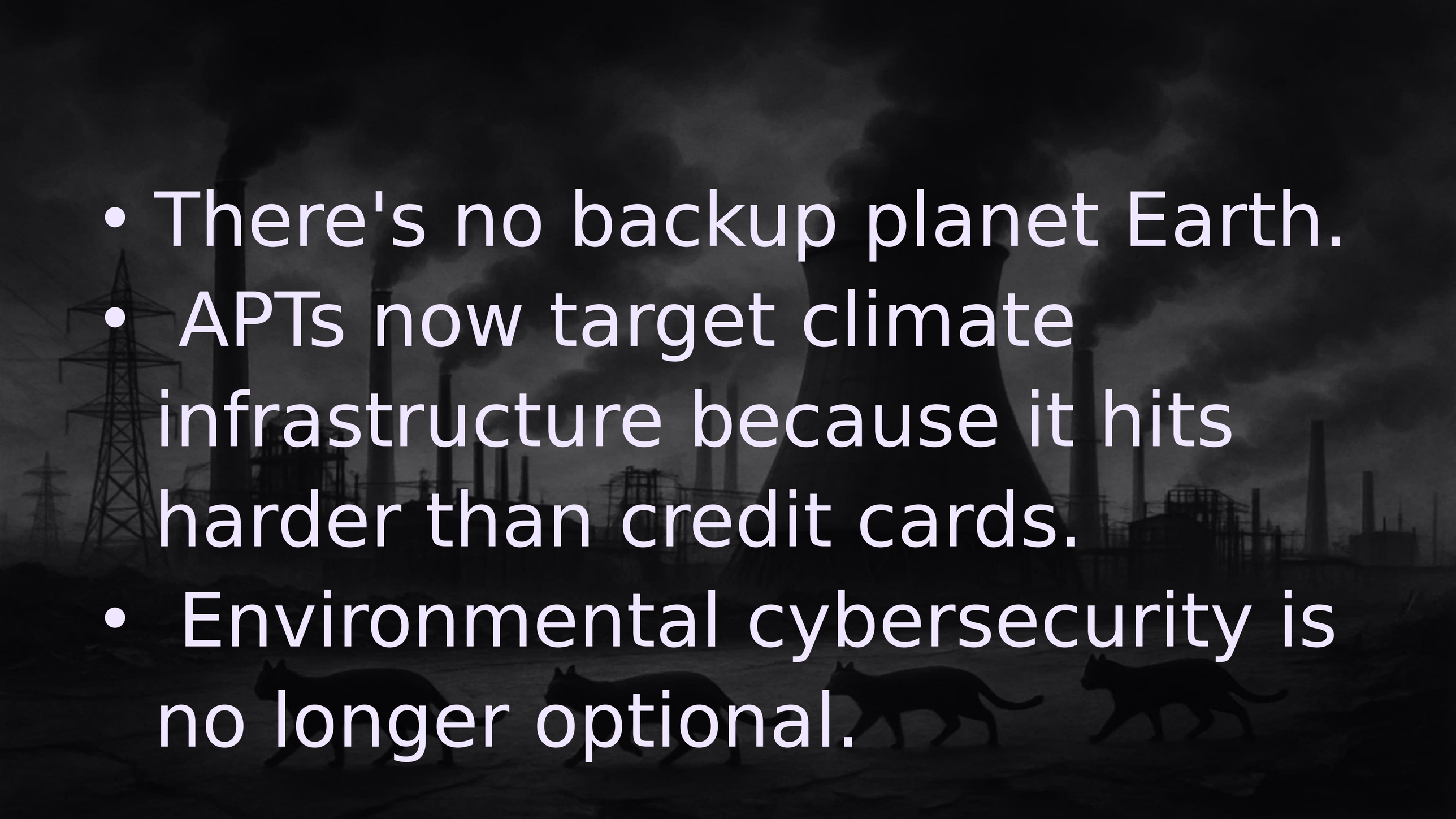
```go
package main
func OptimizeClimateDestruction(targets []string) string {    if CalculateMaxDamage().IsOptimal() {        LaunchCoordinatedAttack(targets)        MaximizeEnvironmentalDamage()        MinimizeDetectionProbability()    }    return "Climate successfully f*cked"}func CalculateMaxDamage() VulnWindow { return VulnWindow{} }func LaunchCoordinatedAttack([]string) { /* chaos */ }func MaximizeEnvironmentalDamage() { /* planet.exe crashed */ }func MinimizeDetectionProbability() { /* stealth mode */ }type VulnWindow struct{}func (VulnWindow) IsOptimal() bool { return true }
```

Next-Generation Environmental Targets

Hydrogen Infrastructure: Production, storage,
distribution control systems
Carbon Capture Systems: Direct air capture
facilities, storage networks
Desalination Networks: Water security infrastructure during droughts
⚛ Fusion Power Plants: Next-generation clean


By the next years, environmental warfare will eclipse traditional cyber operations as dominant nation-state conflict


Don't Just
Stand There



- There's no backup planet Earth.
- APTs now target climate infrastructure because it hits harder than credit cards.
- Environmental cybersecurity is no longer optional.


REMEMBER:
WAR IS BAD FOR KITTENS



THANK YOU

IN/CyberneOliveira/

X/@CharmingMichi

@BadSister@defcon.social

lavillahacker.com