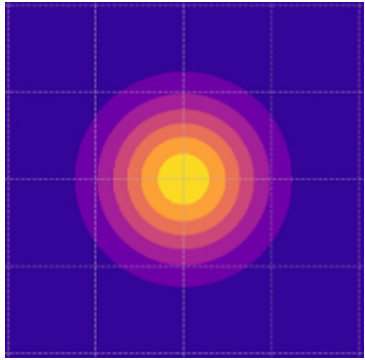




NIST SPECIAL PUBLICATION 800- 239 IPD BUG BASH

JANUARY N. WALKER
PLANETARY INFORMATION
SECURITY OFFICER

THE GREAT SALT LAKE, UTAH



NIST ACKNOWLEDGEMENTS

A High-Performance Computing (HPC) Driven Approach explicitly acknowledges the following:

- 1 Section 5: "Currently, there is a lack of established standards, guidelines, and best practices specifically for AI data center security."
- 2 Section 1: "This publication aims to lay the groundwork for creating security guidelines specific to the computing environment."
- 3 Section 1: "**Comprehensive security for an AI data center must also consider other elements beyond the scope of this document.**" The document explicitly defers physical site perimeter, building and physical infrastructure, operational technology managing power and cooling, and supply chain and personnel operations to a correlative initiative.



Sections 2.2.3, 2.2.4 3.4, 3.5, 3.6, 3.8, 3.10, 3.12, 3.13, 3.13.2 acknowledge attack surfaces within scope but 800-239 provides no physics-derived thermal framework of SMART Benchmarks to address them, an outstanding product requirement. This submission aims to do so and bridge data and power.

JANUARY N. WALKER

UPDATE DEFINITIONS

A case for updating definitions in NIST Special Publication 800-239 ipd

For a standards body like NIST, computable definitions are the ones that can be tested, audited, and enforced. A bit defined only as "a binary digit" tells you what it represents. A bit defined to include $\log_2(2) = 1$ and $\ln(2) = 0.693147$ tells you the physical cost through $E = kBT\ln(2)$, which is what data security requirements can be built on. **As NIST Special Publication 800-239 ipd calls for benchmarks, now is an appropriate time to define.**

Here's why:

1. NIST standards are used across federal agencies, contractors, and regulated industries simultaneously. **Consistency of interpretation across that many organizations requires mathematics, not language.** Language diverges across readers. Mathematics does not.
2. NIST standards are used as the basis for audits, certifications, and legal compliance determinations. A standard that cannot be computed cannot be audited with precision. **A standard grounded in physical law can be independently traced and verified by any party with access to the relevant measurements.**
3. NIST's own mission statement commits it to measurement science. A security standard that cannot be measured is not aligned with that mission. **Adding mathematics to definitions is what makes a standard consistent with what NIST commitment to measurement science.**

DATA ECOSYSTEM

Every device here processes information by flipping bits. Every bit flip dissipates heat and uses storage space as a physical law, as such the following mathematics applies to all computers.



DATA CENTER

Data centers are like thousands of computer hard drives running continuously creating heat islands.



COMPUTERS

The computer retrieves those bits from storage; executes them every operation dissipates heat.



HARD DRIVE

Every code which executes is stored on disk as binary or metadata before a single computation runs.



BIT / CODE

Code instructions are bit patterns and every line run is a bit flipped.

DEFINITION OF A BIT

The definition of a Bit today is founded in language, not mathematics preventing full auditability, and SMART Benchmarking.

Current Bit Definition:

A binary digit: 0 or 1.

Revised Bit Definition:

A bit is a physical distinction in a binary ($p=2$) system representing one of two distinguishable states represented by 0 or 1.

For $p=2$:

- $\log_2(p) = 1$
- $\ln(p) = \log_2(p) / \log_2(e) = 0.693147$

The definition extends to any prime-dimensional system where p is any prime, with $\ln(p) = \log_2(p) / \log_2(e)$ defining the information content of each prime basis state, opening the door for a series of standardized data architectures.

LANDAUER'S DISCOVERY

Landauer discovered bits are not abstract or simply a 1 or a 0. A bit is physical with a minimum energy cost and creates a byproduct of heat, entropy, CO₂, and storage simultaneously. $E = kBT \ln(2)$ is the equation of heat at binary or simply stated, data.



0110
1001
1010



kBT

$\times$

$\ln(2)$

$=$

INFORMATION -
ENERGY

Thermal energy at
temperature T across any
scale.

Entropy applied to two
equally probable binary
states.

The minimum energy required
to cause physical change when a
binary decision becomes data.

DEFINED DEFINITION OF A DATA



Add the following Definition of Data to NIST as there is no definition of data today.

Current Data Definition:

None

Defined Data Definition:

Data is the physical instantiation of an informational distinction in a substrate at temperature T . Its existence requires the irreversible commitment of one physical state, defined by paying a minimum thermodynamic cost of $E = kBT\ln(p)$ per bit. Data cannot exist without the Landauer cost being paid and is the connection between information-energy.

For $p=2$:

- $E = kBT\ln(p)$

* p may be any prime, enabling architecture-agnostic standards applicable to classical, quantum, and hybrid computing systems.



HEAT ON REPEAT

A byte is not just an 8-bit state of 1's and 0's, it is a package of $8 \cdot E = kBT \ln(2)$, and we have not been on the 8-bit system in quite some time. We went through 8-bit, 16-bit, 32-bit, and are now on 64-bit. Each of data packet uses energy AND space simultaneously.

   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$

   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$

   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$

   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$

   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$

   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$

   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$

   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$

   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$

   $E = kBT \ln(2)$

   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$

   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$

   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$

   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$

   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$

   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$

   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$

   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$
   $E = kBT \ln(2)$

BIT

Every 0 and 1 has an information-energy, heat, entropy, and CO₂ cost.

8 BIT BYTE

8-bit flips is 8 minimum energy costs at Landauer.

64 BIT

On a 64-bit system the processor commits the entire word, paying the information energy cost across all 64 positions regardless of how many bits changed.

JANUARY N. WALKER

DATA IMPACT ON WATER

A 64-bit byte CPU executes roughly 10^{-9} -word operations per second. One drop evaporates in about 63 seconds of sustained single core computation at full pipeline cost.

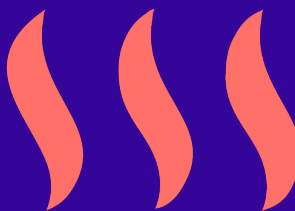
The full heat- pipeline includes Memory access, Storage read/write, Network transmission, creating Cooling overhead for all computers Hardware. To avoid evaporating water, we need to understand the problem of data impact on ecosystems through information physics.

1


$$E_{64} = kBT \ln(2) \times 10^8 \times 64$$

One Byte

2


$$E_{64} = 1.79 \times 10^{-11} \text{ J}$$

Creates Heat
Through full
Computer Pipeline

3



Resulting in one
drop of water
evaporating about
every 63 seconds.

DEFINING DATA AS PHYSICAL

Defining data as physical is important for security

Every security control in NIST SP 800-239 is designed to protect data. If data is defined only as an abstract or logical concept, the security requirements built on that definition have no physical grounding. They describe protections for something whose physical nature is unspecified.

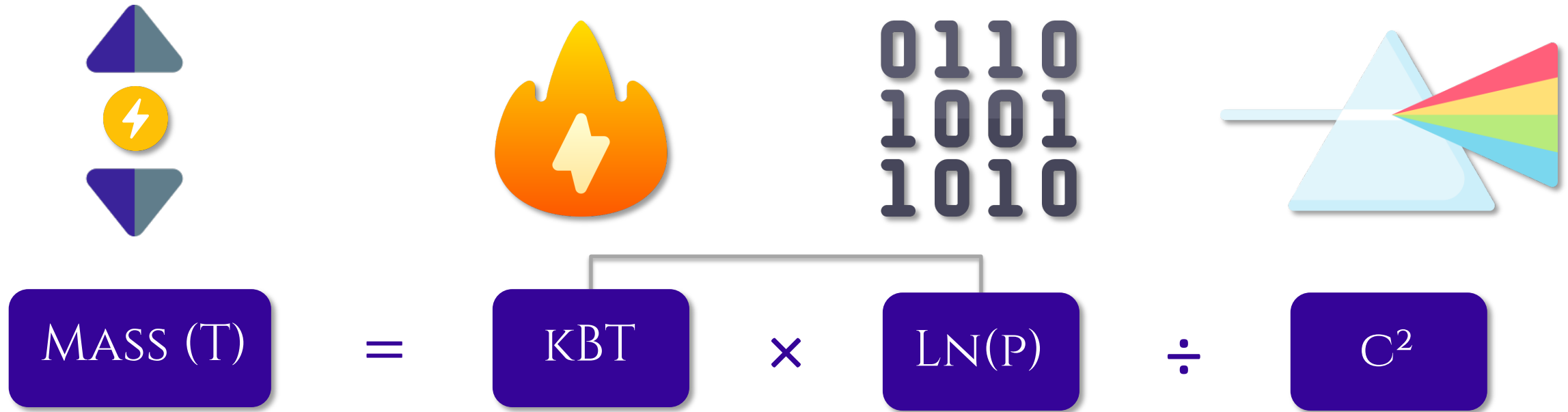
If data is defined as physical, three things follow which matter for security:

1. **Data has a location.** It exists in a specific physical substrate at a specific temperature. That location is auditable.
2. **Data has a cost.** $E = kBT \ln(2)$ per bit was paid to create it. That cost is measurable in the thermal and power telemetry of the facility.
3. **Data has an identity.** Its creation, movement, and destruction all produce thermodynamic signals that are physically present whether or not any software monitoring layer is watching.

A security standard built on a physical definition of data can be audited, measured, and verified independently of software and connecting to the larger ecosystem. A security standard built on an abstract definition of data can only require software attestation, which can be falsified.

MASS-ENERGY-INFORMATION

Defining data as physical through $E = kBT \ln(p)$ enables Melvin Vopson's mass-energy-information equivalence $m(T) = kBT \ln(p)/c^2$ at $p = 2$ to derive with algebra three verifiable properties of data in any classical, AI, or quantum system.



Identity: information mass $m(T)$ is distinct and computable at operating temperature providing an **Infoton** identity.

Location: data exists at temperature T in a specific physical substrate

Cost: minimum thermodynamic cost $E = kBT \ln(p)$ per bit is measurable from thermal telemetry

DEFINED DEFINITION OF INFOTON

Add the following Definition of Information mass to NIST as there is no definition of information particles today.

Current Infoton Definition:

None

Defined Infoton Definition:

The Infoton is a framework for deriving the information-energy properties of physical systems. Its mass equation $m(p, T) = kBT \ln(p)/c^2$ connects Einstein's $E = mc^2$ to Landauer's $E = kBT \ln(2)$ and extends to any prime p . From a single measured mass, it derives with zero free parameters:

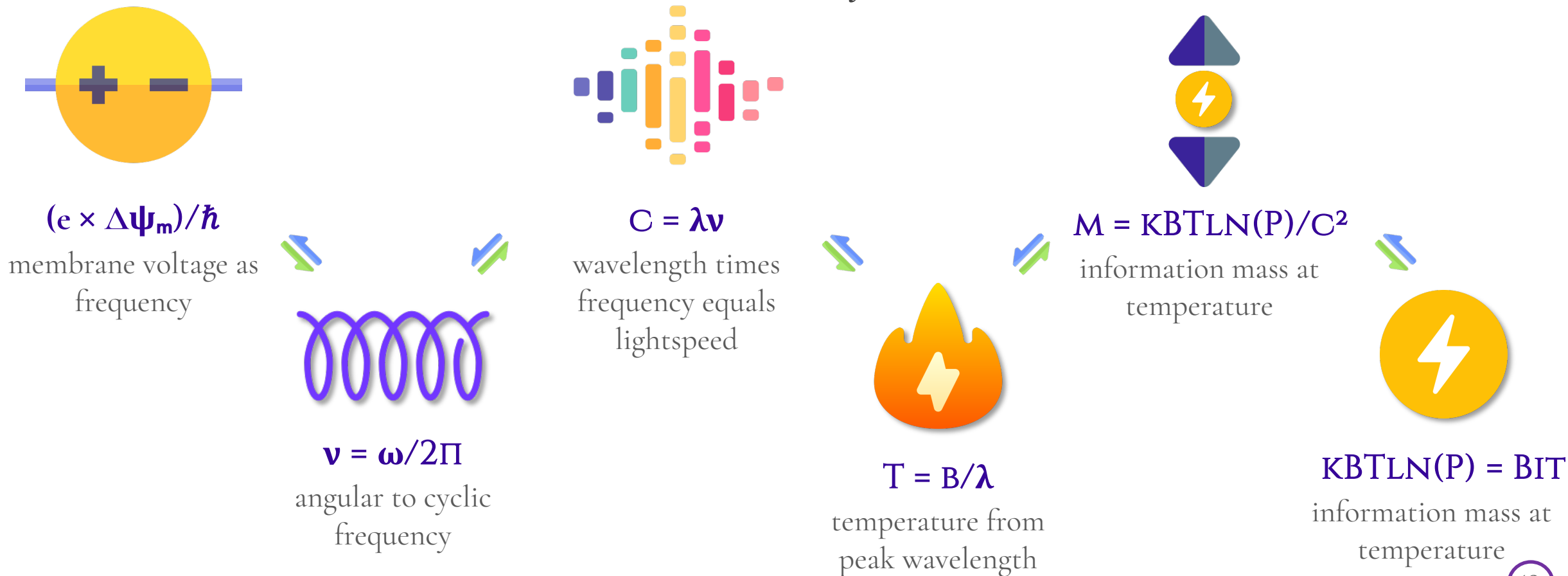
For $p=2$:

- $m(p, T) = k_B T \ln(p) / c^2$
- Identity: $\log_{10}(T) = \log_{10}(m) + 39.9727$ at $p=2$

* p may be any prime, enabling architecture-agnostic standards applicable to classical, quantum, and hybrid computing systems.

SMART INFOTON BRIDGE

This chain connects electromagnetic frequency through temperature through information mass through Landauer energy to the bit creating a bridge to SMART benchmark functionality.



INFORMATION PHYSICS TOOLS

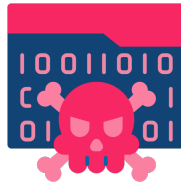
For Data Security the following tools must be defined, benchmarked and utilized to protect Information Ecosystems. Add the following to NIST Special Publication 800-239 ipd



$$AF = \exp[(E_a / k_B) \times (1/T_1 - 1/T_2)]$$

ARRHENIUS ACCELERATION FACTOR

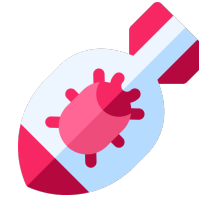
Hardware failure rate at
operating temperature



$$H(X) = -\sum P(X) \times \log_2(P(X))$$

SHANNON ENTROPY

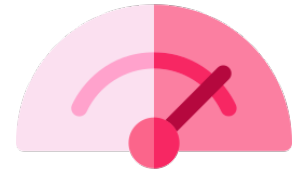
Information disorder and
malware detection baseline



$$\Lambda = \ln(2) / X_{\text{FREQ}} = 0.24567...$$

THE BLACKBODY CONSTANT

Information erasure
position in thermal
radiation field



$$ISM = R_{\text{CONTROL}} \times DP_{\text{MIN}} / N / (DP/DT),$$

INFOTON SAFETY MARGIN

Monitoring system
observability threshold

JANUARY N. WALKER

AI INJECTION ATTACKS

AI/ML Injection attacks through excessive token usage are evidence of either poor coding quality not based in math, or of malware injection attacks and model poisoning.

A core tenant of Data Storage Security is not filling up data centers with code waste (Entropy) which will turn into future unused cold storage draining local heat and energy stores.

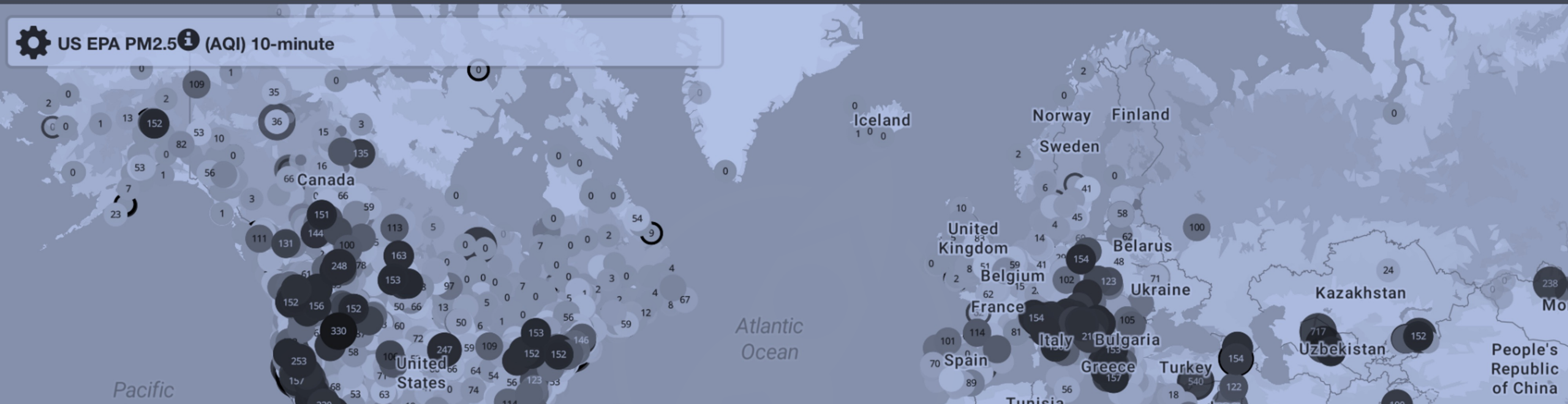
CYBER WARFARE

War extends far beyond our physical actions into data, A DDoS attack is a concentrated energy event — like **dynamite**, its damage is proportional to power delivered per second, not just data volume.

11.5

DDOS ATTACKS REACHED RECORDS IN 2025 EXCEEDING TERABITS PER SECOND.

1. Every DDoS attack has a thermodynamic signature: power draw, heat output, and dm/dt at the target infrastructure
2. Proposed 3-tier auditing chain: data center (LSM, dm/dt , Arrhenius) → energy provider (load anomaly against declared baseline) → regional grid (aggregate demand spikes correlated across multiple providers)
3. A hotspot map built from tier 2/3 telemetry turns isolated attack alerts into a real-time, cross-provider threat picture — detectable before software-layer logs catch up
4. Proposed requirement: energy providers serving data centers above a disclosed load threshold shall report anomalous demand signatures to a shared threat registry, cross-referenced against LSM/ dm/dt disclosures from Section 4.2 in real time.



Data Cybersecurity parameters are detectable through environmental benchmarks as information produces measurable impacts like excessive heat, poor air quality, and ecosystem noise pollution.

Unexplained Regional
Heat from DDOS
evaporating bodies of
water.

Noise Pollution from
machines produces detectable
noise from overworked fans

Poor air quality from heat
waste and imprecise machine
design impacts neural
functions

SMART INFORMATION PHYSICS

Based on the bug bash, the following equations are proposed as SMART Benchmarks grounded in information physics for the identified attack surfaces in NIST SP 800-239.

▶ **Section 2.2.3:** $E = kBT \ln(p)$

▶ **Section 2.2.4:** $E = kBT \ln(p)$, $dm/dt = P/c^2$

▶ **Section 3.4:** $ISM = R_{\text{control}} \times dP_{\text{min}} / N / (dP/dt)$, $\Lambda = 0.24567$

▶ **Section 3.5:** $ISM = R_{\text{control}} \times dP_{\text{min}} / N / (dP/dt)$, $H(X) = -\sum P(x) \times \log_2(P(x))$

▶ **Section 3.6:** $ISM = R_{\text{control}} \times dP_{\text{min}} / N / (dP/dt)$, $H(X) = -\sum P(x) \times \log_2(P(x))$, $dm/dt = P/c^2$

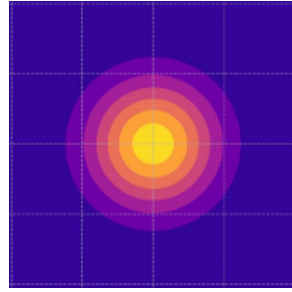
▶ **Section 3.8:** $dm/dt = P/c^2$, $m(T) = kBT \ln(2)/c^2$

▶ **Section 3.10:** $AF = \exp[(E_a/kB) \times (1/T_1 - 1/T_2)]$

▶ **Section 3.12:** $dm/dt = P/c^2$, $ISM = R_{\text{control}} \times dP_{\text{min}} / N / (dP/dt)$

▶ **Section 3.13:** $\Lambda = 0.24567$, $E = kBT \ln(p)$

▶ **Section 3.13.2:** $\Lambda = 0.24567$, $E = kBT \ln(2)$, $AF = \exp[(E_a/kB) \times (1/T_1 - 1/T_2)]$



PROPOSAL

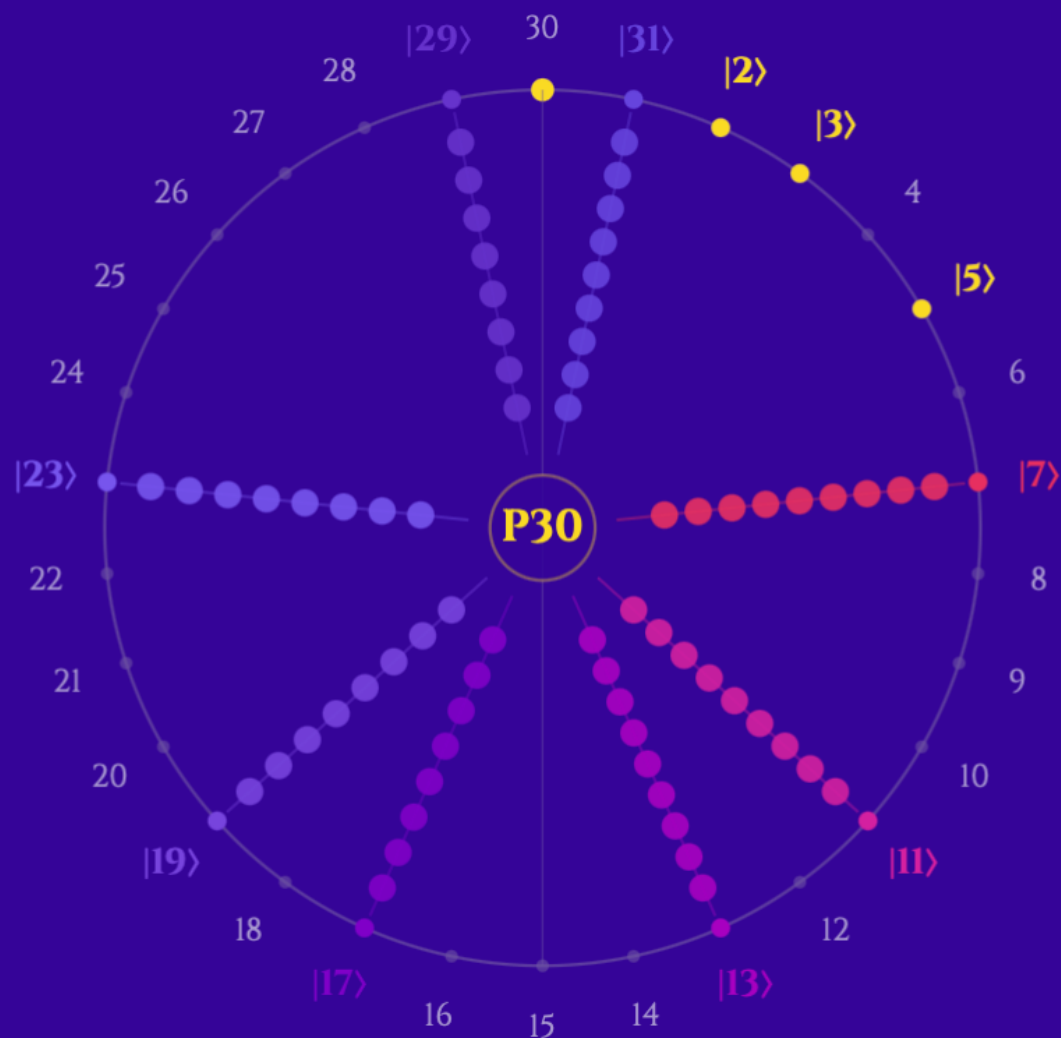
It is proposed to explore data improvements which meet the following product requirements.

1. Compatible with 8-bit architecture and computers today
2. Reduced energy usage and data storage
3. Compatible with quantum architectures.

It is noted Euler $\varphi(p)$, $p = 30$ matches all 3 requirements. An example architecture is provided which functions with $m(T) = kBT \ln(p)/c^2$. **P30 Demo available.**

"The Great Salt Lake can be fully restored to full health within as little as 3 years by returning 1,150,000 AF/yr. Resulting Utah's lake effect and water security." - January Walker

163 CHARACTERS · 489 OPERATIONS · 167 POSITIONS



Ingress encode complete. All 163 characters became coprime positions, once. Now press Play again to read the data back. The value is already a position, so reading it costs nothing. Watch the count stay flat.

OPERATIONS, BIOS-NATIVE

Re-verify on read

0

Ingress encode

163

Total P30

163

BIOS mode: encode happens once, as data enters the machine. After that the value stays a coprime position through every layer, so reads cost nothing and validity holds by construction.

STORAGE, VERIFIED AGAINST THE CODEC

UTF-8 baseline

163 BYTES

P30 positions (CHAR)

167

CHAR mode, round-trips

167 BYTES

PACKED mode, round-trips

171 BYTES

HUFFMAN total, round-trips

533 BYTES

HUFFMAN payload only

103 BYTES

DIRECT packed, write-only 116 BYTES

At short lengths P30 is not about making files smaller; on this sentence it is within a few bytes of UTF-8. What it buys instead is built-in integrity: the data carries its own correctness, so no separate error-correction layer has to be stored or maintained alongside it. The size advantage arrives on longer data; the integrity advantage is there from the first

“The Great Salt Lake can be fully restored to full health within as little as 3 years by returning 1,150,000 AF/yr. Resulting Utah's lake effect and water security.” — January Walker

163 CHARACTERS · 1,304 BITS · 21 WORDS OF 64 BITS

BYTE 0 → T

O

I

I

I

O

I

O

O

BYTE 1 → Y

O

I

I

I

I

O

O

I

BYTE 2 → .

O

O

I

O

I

I

I

O

BYTE 3 → _

O

O

I

O

O

O

O

O

BYTE 4 → _

O

O

I

O

O

O

O

O

BYTE 5 → _

O

O

I

O

O

O

O

O

BYTE 6 → _

O

O

I

O

O

O

O

O

BYTE 7 → _

O

O

I

O

O

O

O

O

8 CHECK BITS

Hsiao (72,64)

C0 watches 26

I

C1 watches 26

O

C2 watches 26

O

C3 watches 26

I

C4 watches 26

O

C5 watches 26

I

C6 watches 26

O

C7 watches 26

I

the 9th byte: pure overhead

Whole tweet verified: 21 words, 12,264 operations, every one of them spent only to confirm the message did not change. P30 63. would have finished in

OPERATIONS PERFORMED

Write overhead2688

Read overhead9576

Total ECC12264

STORAGE TAX

Data delivered64 BITS · 8 BYTES

Check bits stored8 BITS · 1 BYTE

Physically stored72 BITS · 9 BYTES

Space spent on checks12.5% · 1 BYTE IN 9

A ninth byte of pure overhead rides with every eight. The 8 check bits follow a Hsiao (72,64) matrix^[9]^[10], each covering 26 of the 64 data bits. This 12.5% is the floor for one ECC scheme; real facilities layer replication or erasure coding on top^[11]. It is a storage tax, separate from the per-access energy cost.

LANDAUER ENERGY FLOOR

Operating temperature

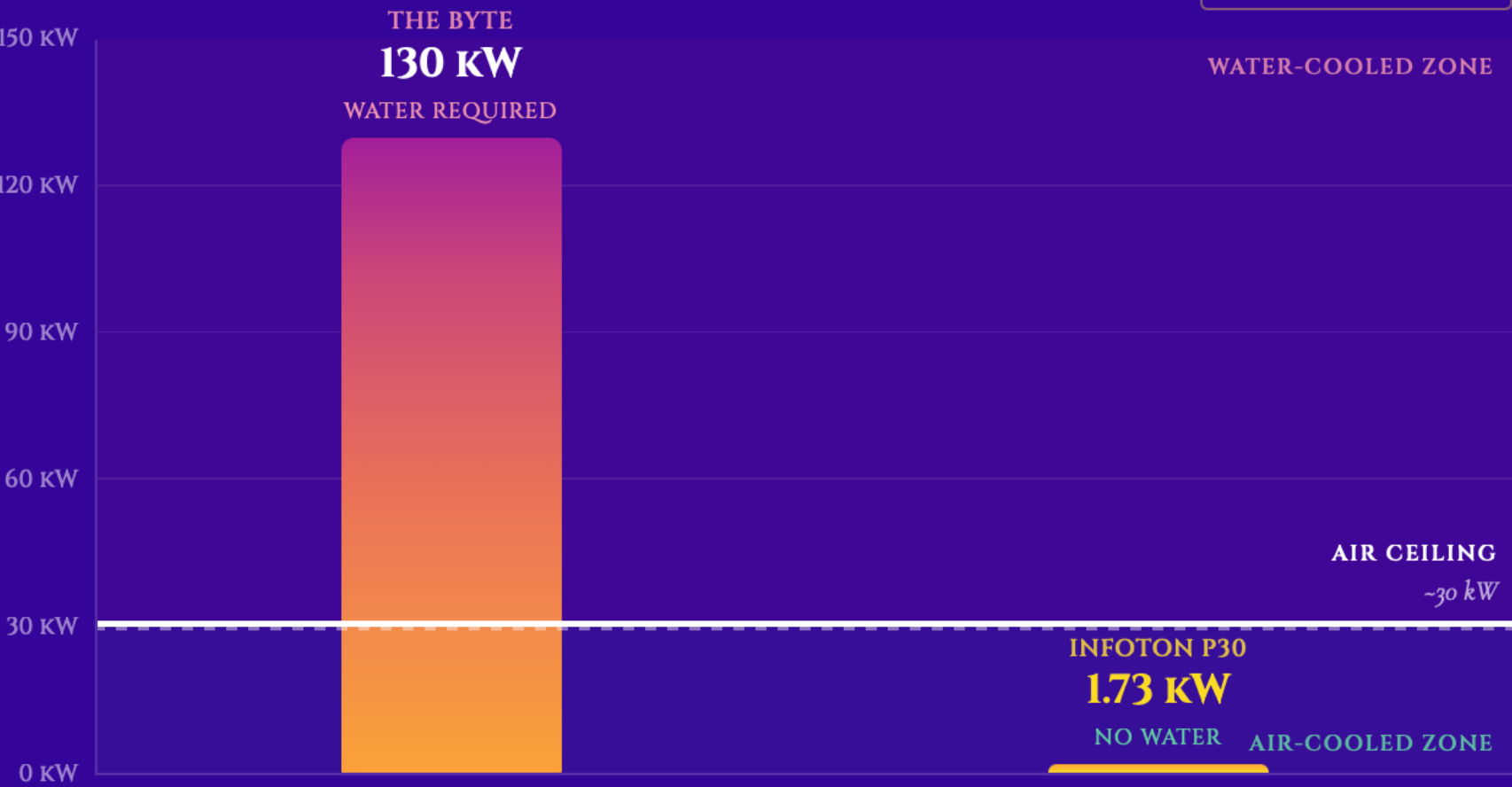
350 K · 77°C (typical DRAM junction)↕

Per operation3.349 ZJ

This run (12264 ops)41.078 AJ

$E = k_B T \ln(2)$ per irreversible operation. The floor rises with temperature: hotter silicon means a higher thermodynamic minimum, before any real switching loss.

HEAT PER RACK VS THE AIR CEILING



130 KW → 1.73 KW

The byte's column towers 4.3× above the ceiling: the heat it dumps per rack cannot be carried by air, so liquid and evaporative water are forced on. P30 delivers the identical message and never reaches the line.

THE MATH, STEP BY STEP

- 1 Operation ratio = 12,264 / 163 = 75.2×
P30 reaches the same result in 75.2× fewer irreversible operations.
- 2 Power scales linearly: $P = N \times ops \times E_{op}$
Same throughput N, same silicon E_{op} : only the op-count differs.
- 3 P30 rack power = 130 kW × (163 / 12,264) = 1.73 kW
The byte's 130 kW load, recomputed at P30's op-count.
- 4 No-water: 1.73 kW ≤ 30 kW air ceiling ✓
Byte: 130 kW > 30 kW → water required. P30: 1.73 kW < 30 kW → air only.
- 5 Threshold: $N^* = Q_{air} / (ops \times E_{op})$ rises 75.2×
P30 tolerates 75.2× the throughput before any water is ever needed.

OPERATIONS PER MESSAGE

Byte + Hamming ECC	12,264
Infoton P30	163

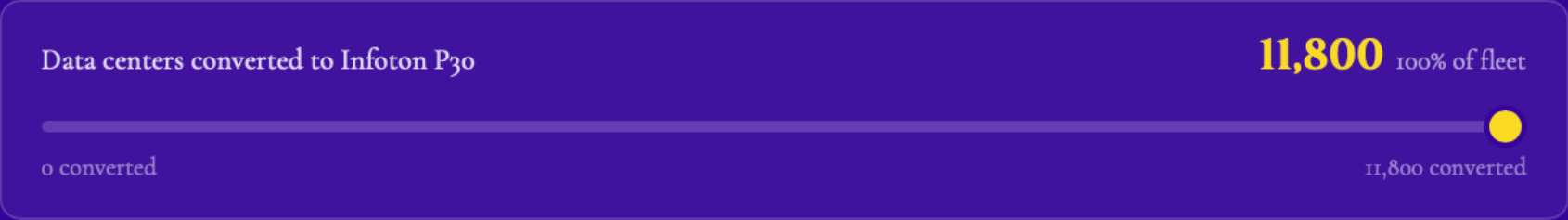
No-water condition: $P(N) = N \times ops \times E_{op} \leq Q_{air}$. Threshold: $N^* = Q_{air} / (ops \times E_{op})$. Cutting ops from 12,264 to 163 raises N^* by exactly 75.2×.

UNITED STATES · 5,500

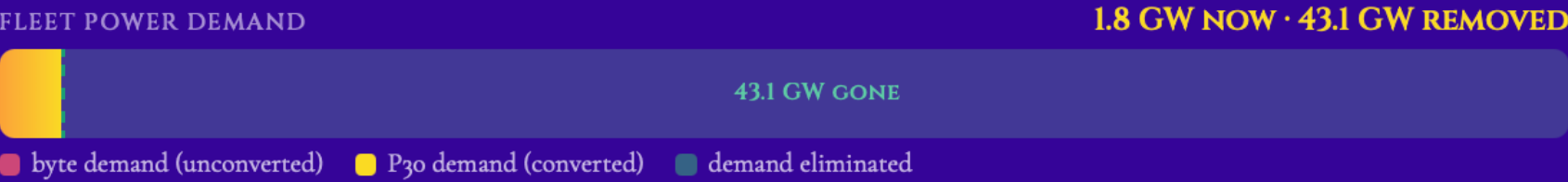
GLOBAL · 11,800

UTAH · 13 REACTORS

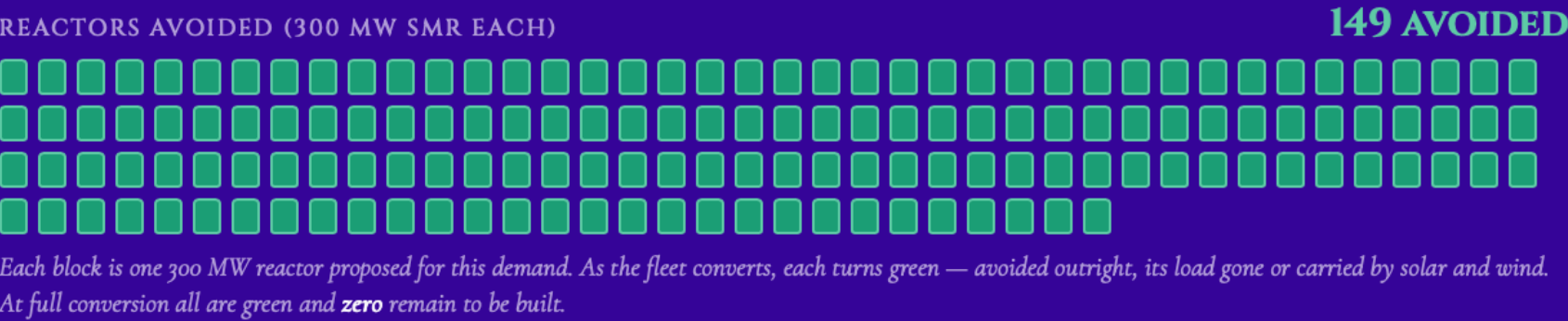
43.1 GW SAVED



FLEET POWER DEMAND



REACTORS AVOIDED (300 MW SMR EACH)



WASTE HEAT EJECTION STOPPED



Full conversion: the entire global fleet runs on the Infoton. Demand falls by 43.1 GW, 149 SMRs are never built, and the remainder is served by wind and solar without extracting new fuel.

REACTORS NEEDED FOR THIS DEMAND

GLOBAL, AT THIS DEPLOYMENT

0

all 149 proposed reactors avoided; remainder on solar and wind

AT THIS DEPLOYMENT LEVEL

Converted 11,800 / 11,800

Fleet demand now 1.8 GW

Demand eliminated 43.1 GW

Energy avoided / yr 377 TWH

Waste heat stopped 43.1 GW

SMRs avoided 144

1 GW reactors avoided 43.1

WASTE HEAT STOPPED

HEAT EJECTION ELIMINATED

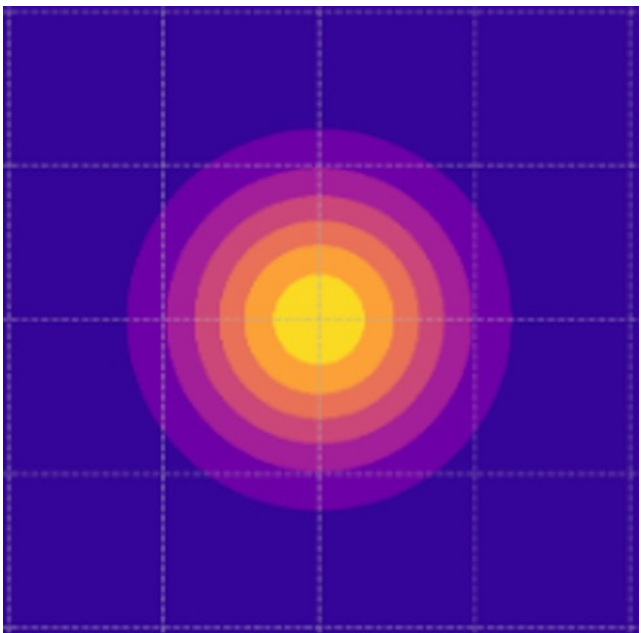
43.1 GW

thermal, no longer dumped to air and water

Annual waste heat avoided 377 TWH

Equivalent homes heating 33.9 M

Water warmable by 1°C 0.32 KM³



INFOTON

SAVE SPACE

WHO IS JANUARY?

JANUARY N. WALKER is the Planetary Information Security Officer and operates **INFOTON**, an Information Physics company specializing in particles of data, cybersecurity, and information systems at the seam of Biology.

She has extensive full stack career experience in Product Management, Cybersecurity, & Information security, serving as an Information Security Officer of cryptography at major financial institutions and as a product manager leading major initiatives grossing in the millions & billions. Her notable work includes leading the first digital identity system, sovereign identity, and enhanced digital identity with behavioral biometrics and machine learning algorithms at the core of AI to verify human presence and authenticity in critical transactions.

Recognizing emerging threats in intelligence, social engineering, quantum computing, and brain-computer interfaces, Walker expanded her expertise into neuroscience and information physics to develop protective frameworks for information systems. She designed the **Cybersecurity Mindfulness** program to protect from social engineering in social and AI systems beyond phishing.

January N. Walker is available for consult on all systems and government structure connected to Information and can be reached at January@infoton.ai

