NISTIR Metrology 6025 Information Physics Mapping

January N. Walker
Planetary Information Security Officer



The Great Salt Lake, Utah

Objectives

NIST is the National Institute of Standards and Technology, Information Technology (IT) lacks a metrology linking information physically to SI. Information Physics is the link.



1. Derive the metrology of information from established Information Physics.
2. Bridge Information Physics mathematics to known SI measurement.
3. Define “data” from the mathematics of Information Physics.

NIST Acknowledgements

NISTIR 6025 from 1993 explicitly acknowledges the following

1. **Preface (p.1)** The task group reports "it did not find any previous work addressing metrology for IT." **No IT equivalent of ISO 1000 or ISO 31.**

2. **Units and Scales (p.7):** NISTIR 6035 says **calling a bit a unit of measure meant is not valid without specifying which quantity is being measured.** NISTIR 6025 notes the bit has been used to measure optical resolving power.

3. **Footnote (p.10):** SI itself states that it does not treat information as content, and suggested **Shannon and Weaver may sufficiently characterize information as a quantity and the bit as it's unit.**

4. **Uncertainty (pp. 10, 18):** Physical metrology methods for expressing uncertainty cannot easily be be applied**, uncertainty for software described as genuine frontier.**

5. **Opportunities (p.20):** NISTIR 6025 **asks whether IT needs an expanded system of fundamental and derived units** while leaving the question open.

6. Conclusions (p.21): IT metrology is described as a valid branch of metrology, and **NISTIR 6025 concluded SI dimensioning system was less relevant to IT [☹].**



- NISTIR 6025 treats quantities, units, and scales as a consensus process with some arbitrariness (p.7). Each quantity follows from physical constants

Metrology Definitions

A case for updating definitions in NIST to be founded in derived Metrology

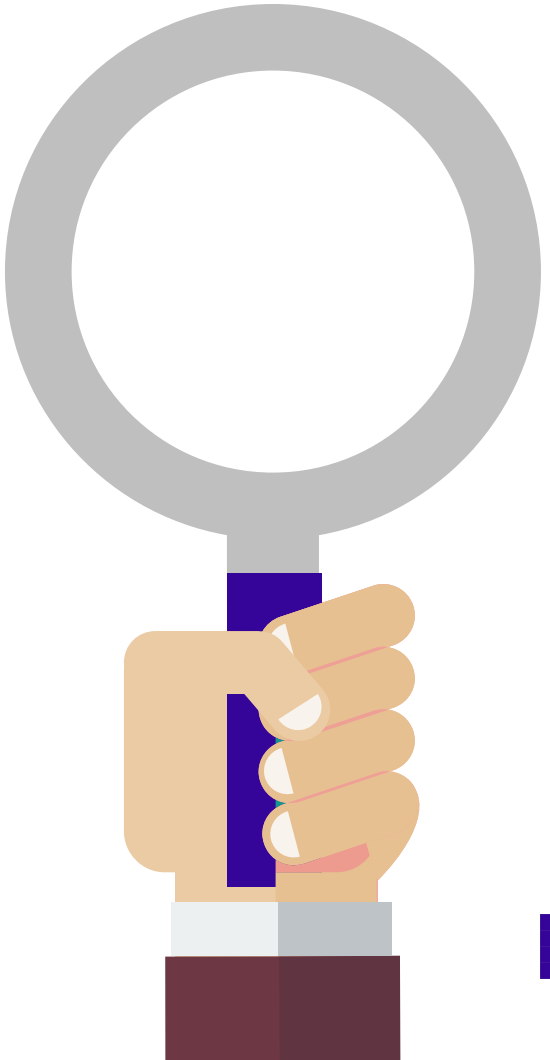
As a standards body, computable definitions are the ones that can be tested, audited, and enforced. A bit defined only as "a binary digit" tells what it represents. A bit defined to include $\log_2(2) = 1$ and $\ln(2) = 0.693147$ tells the physical cost through $E = kBT\ln(2)$, which is what data security requirements can be built on. AI Data Centers consume electricity, water, and heat that are measured in SI, yet the information they process is reported in units with no definition, with no defined link, the impact cannot be verified. The SI-IT link is kB.

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 physics derived mathematics to definitions is what makes a standard consistent with NIST commitments to measurement science.

Accountability Framework

Benchmarking requires something to be accountable against. In mature fields a measured quantity has a reference. Where the reference is missing, a failure can be made and not attributed.



1. **Defined Quantity.** Without a defined quantity there is no accountability. “Uptime,” ”capacity,” “throughput,” ”compute,” are vendor defined so a dispute has no neutral referent.

2. **A Reference.** Without a primary standard, two measurements of the same thing cannot be reconciled. The disagreement is between two benchmarks, with no arbiter.

3. **Traceability.** Auditors need an unbroken reference from a reported number back to a standard.

4. **Stated Requirements.** An energy-information quantity anchored to physical constants allows data performance to be stated as a value with a benchmark.

A regulator can set a limit only on something measurable. Where the quantity is undefined, the rule cannot be enforced.

Derived Metrology

Information Physics provides a framework which defines the physical quantity first, then derives its unit from the constants

Derivation is Traceability

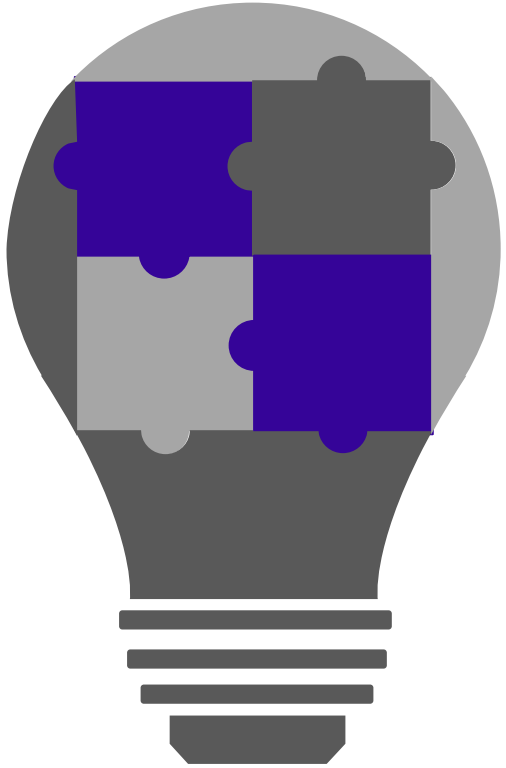
Instead of tracing data to a entity definition or committee convention, each quantity traces to constants (kB, h, c, T) through stated derivation.

Data Definition is Unit

The base of the logarithm (bit vs natural unit of measurement) is stated as part of the derivation.

Uncertainty in Constants

Constants carry known uncertainties (kB, h), a derived quantity has a computable uncertainty budget.



Physics Native Accounting

Energy per bit, heat per operation, and thermal limits are outputs of derivation instead of empirical add-ons.

Security and Trust Quantified

Energy leakage, and assurance benchmarks can be derived in a from entropy measurement instead of asserted through conformance.

Measurable referent

Regulators can set a limit from a information physics derived definition and stated realization.

The 1997 NISTIR 6025 paper states the bit is not a valid unit until the quantity is specified.

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.



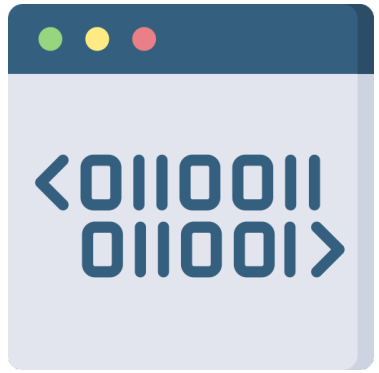
Computers

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 very line run is a bit flipped.

Metrology of a Bit

0110
1001
1010

the "bit" is a unit of measure in IT is not valid without specifying what quantity is being measured." – NISTIR 6025

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 information-energy states represented by 0 or 1.

For p=2:

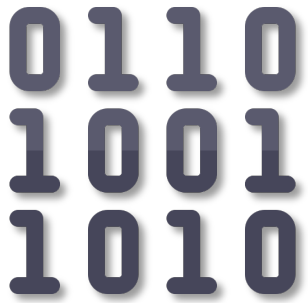
- $\log_p(p) = 1$
- $\ln(p) = \log_p(p) / \log_p(e) = 0.693147$

The definition extends to any prime-dimensional system where p is any prime, with $\ln(p) = \log_p(p) / \log_p(e)$ defining the information content of each prime basis state, opening the door for a series of standardized metrology in data architectures. **Prime states have quantum relatives.**

Landauer's Discovery

Landauer (1961) 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, CO_2, and storage simultaneously. $E=kBTln(2)$ is the equation of heat at binary or simply stated, **metrology**.







kBT × **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 **information**.

* Bérut proved Landauer in 2012.

Metrology of Information

Add Landauer Definition of Information -Energy to NIST as there is no definition of Information-Energy today.

Current Data Definition:

None, 11 conflicting definitions, none of which are mathematical or based in physics.

Defined Information-Energy Definition:

Landauer 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 = kBTln(p) per bit. Data cannot exist without the Landauer cost being paid and is the connection between information-energy.

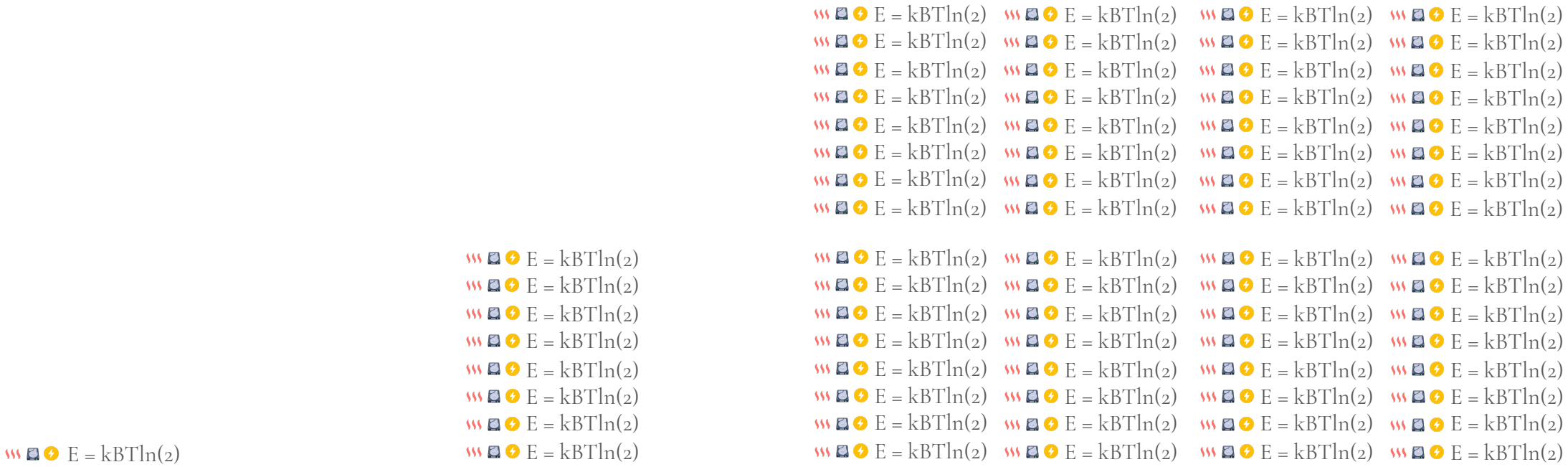
For p=2:

- **E = kBTln(p)**

* p may be any prime, enabling architecture-agnostic computing standards applicable to classical, quantum, and hybrid computing systems in both byte and alternative data architectures.

Heat on Repeat

A byte is not just an 8-bit state of 1's and 0's, it is a package of 8-E = kBTln(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 byte packet uses energy AND space simultaneously.



Bit

Every 0 and 1 has an information-energy, heat, entropy, and CO_2 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.

Byte 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.

1



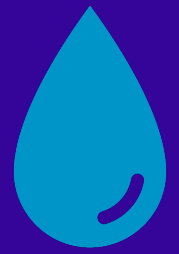
$E_{64} = kBT\ln(2) \times 10^{8} \times 64$
One Byte

2



$E_{64} = 1.79 \times 10^{-11}$ J
Creates Heat
Through full
Computer Pipeline

3



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

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. For example, an email evaporates a glass of water.**

Defining Data as Physical

Defining data as physical is important for security

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.

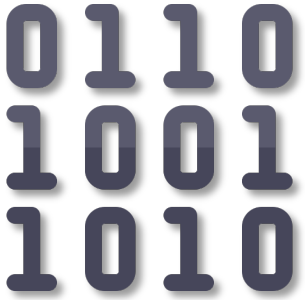
A security standard built on a physical definition of data can be audited, measured, and verified independently of software and connecting to the larger ecosystem. A security standard built on an abstract definition of data can only require software attestation, which can be falsified.

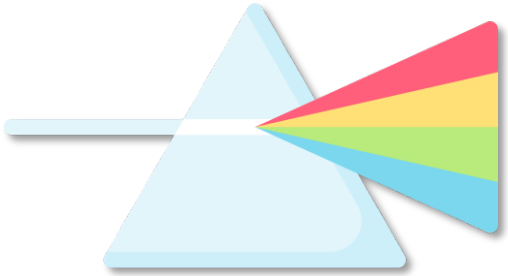
Mass-Energy-Information

Defining data as physical through E = kBTln(p) enables Melvin Vopsons 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, SI, or quantum system.









Mass (T) = kBT × ln(p) ÷ c^2

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 = kBTln(p) per bit is measurable from thermal telemetry

Chemistry Information physics

Through basic algebraic physics Infoton Identity can be derived from chemistry using mass-energy-information equivalence bridging Système International d'unites to Information Technology.

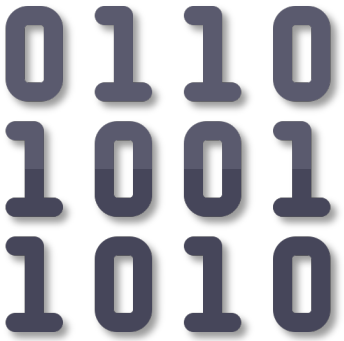
MASS



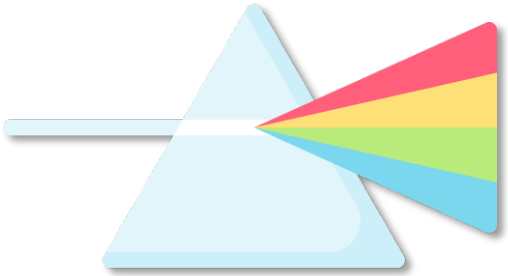
Temperature



DATA



Speed of Light



$$\text{Mass (T)} = \text{KBT} \times \text{LN(P)} \div C^2$$

Metrology of Infoton

Add the following Definition of data to NIST as there is no definition of data 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 $m(p, T) = kBTln(p)/c^2$ connects Einstein's $E = mc^2$ to Landauer's $E = kBTln(2)$ and extends to any prime p. From a single measured mass, it derives with zero free parameters:

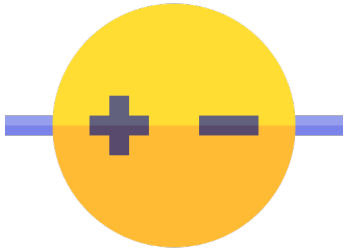
For p=2:

- **$m(p, T) = kB\ T\ ln(p) / c^2$**
- **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.

Information Measurements

This chain connects electromagnetic frequency through temperature through information mass through Landauer energy to the bit creating a bridge to Metrology metrics.



$(e \times \Delta\psi_m)/\hbar$

Membrane voltage as frequency



$C = \lambda\nu$

Wavelength times frequency equals lightspeed



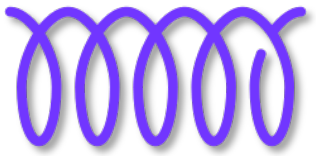
$M(P,T) = KBTLN(P)/C^2$

Data is information mass at temperature



$LOG_p(P) = 1$

Prime dimensional bits



$\nu = \omega/2\Pi$

Angular to cyclic frequency



$T = B/\lambda$

Temperature from peak wavelength



$E = KBTLN(P)$

Information-Energy

Physics Definitions

Each symbol has a mathematic and corresponding meaning in Information Physics

e Elementary Charge	**$\Delta\psi_m$** Membrane Potential Voltage	**$\hbar$** Reduced Planck Constant	**ω** Angular Frequency	**ν** Cyclic Frequency
c Light Speed	**λ** Wavelength	**T** Temperature	**b** Wien Constant	**m** Information-Energy Mass
kB Boltzmann Constant	**p** Prime	**$\log_p$** Base-p Logarithm	**$\ln(p)$** Natural Logarithm	**1** One Prime Bit

Weights and Measures

True regulatory reconciliation requires two independent measurements in a common, certified unit, but data resource consumption is tracked only at the facility level, never at the point of execution, because Landauer has never been recognized as a derived SI standard.

Water

Without SI/IT metrology, facility water meters leave aquifer evaporation untraced to server operations.

Heat

Without SI/IT metrology, building cooling logs leave thermal overhead per operation unmeasured.

Energy/electricity

Without SI/IT metrology, substation power meters leave processing-layer economic energy waste invisible.



Noise

Without SI/IT metrology, property-line noise limits leave fan surges unlinked to processing spikes.

Materials

Without SI/IT metrology, hardware arrival weights leave material costs unallocated to processing.

Air/emissions

Without SI/IT metrology, facility emission tracking remains untraced to server operations.

Speed of Calculations

Reactor Doubling Time in Prompt Criticality



Nuclear Information Systems

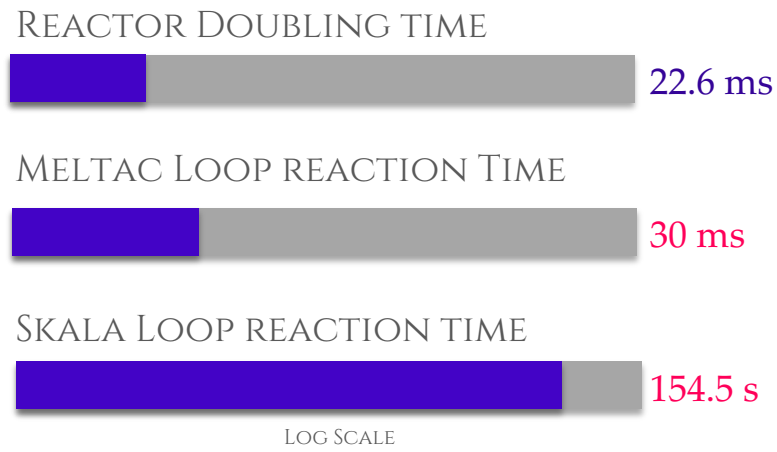
MELTAC Data Architecture is the same as SKALA

Calculations

The reactor doubles its power every 22.6 milliseconds. SKALA took about 155 seconds to respond, roughly 6,800 times too slow. MELTAC takes 30 milliseconds, thousands of times faster than SKALA, but still 1.3 times slower than the reactor. Forty years of improvement shrank the gap but never put the control system ahead of the reactor, and that is a limit of data architecture, not of the engineering.

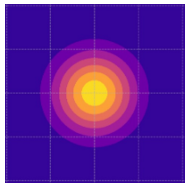
If a reactor enters a prompt-criticality transient, today's byte-based control system cannot respond in time, so safety rests on the reactor's own physics holding, which a beyond-design-basis earthquake would break.

byte-based class limit



To prevent another Chernobyl, Nuclear information systems must respond **faster** than the reactor doubles. No byte class has the Infoton metrology to perform on stated promises. A planetary risk.

No metrology standard exists for Information Technology computation, and the data economy is scaling on thermodynamic, storage, and resource costs uncoupled from the Standards International Unit which no market, regulator, or consumer can verify. The following metrology ground IT to SI reality.



SI ⇄ IT

SI is the International system (Système International d'unités) and the worlds standard framework for measurement. SI and IT are equally relevant and intertwined.

Quantity	Information Physics (IT)	Unit	Symbol
Time	$\tau = h / (4 \times kBTln(p))$	second	s
Length	$\lambda_L = hc/kBTln(p)$	meter	m
Mass	$m(T) = kBTln(p)/ c^2$	kilogram	kg
Electric current	$dQ/dt = e(dE/dt)/(kBTln(p))$	ampere	A
Thermal Temperature	$E = kBTln(p)$	kelvin	K
Amount of Substance	$E_m,min = RTln(p)$	mole	mol
Luminous Intensity	$v_L = kBTln(p)/h$	candela	cd

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



$$AF = \exp[(Ea / kB) \times (1/T1 - 1/T2)]$$

Arrhenius Acceleration Factor

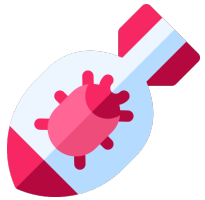
Hardware failure rate at operating temperature



$$H(X) = -\Sigma P(X) \times LOG_2(P(X))$$

Shannon Entropy

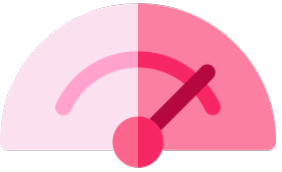
Information disorder and malware detection baseline



$$\Lambda = LN(2) / X_FREQ_ = 0.24567...$$

The Blackbody Constant

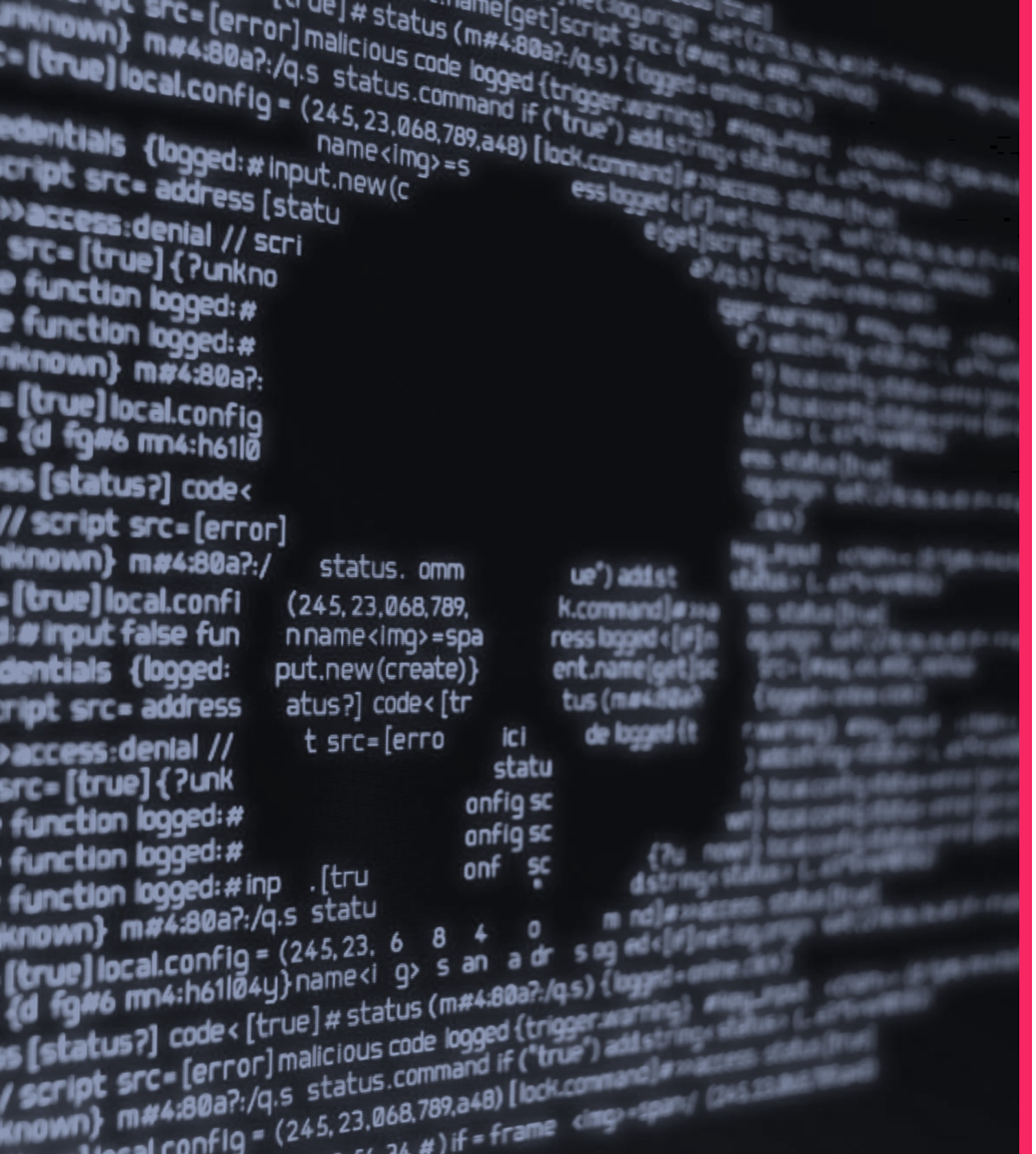
Information erasure position in thermal radiation field



$$ISM = R_CONTROL \times DP_MIN / N / (DP/DT),$$

Infoton Safety Margin

Monitoring system observability threshold



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.



An entropy and machine learning based approach for DDoS attacks detection in software defined networks
August 6, 2024
Scientific Reports, Nature

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.

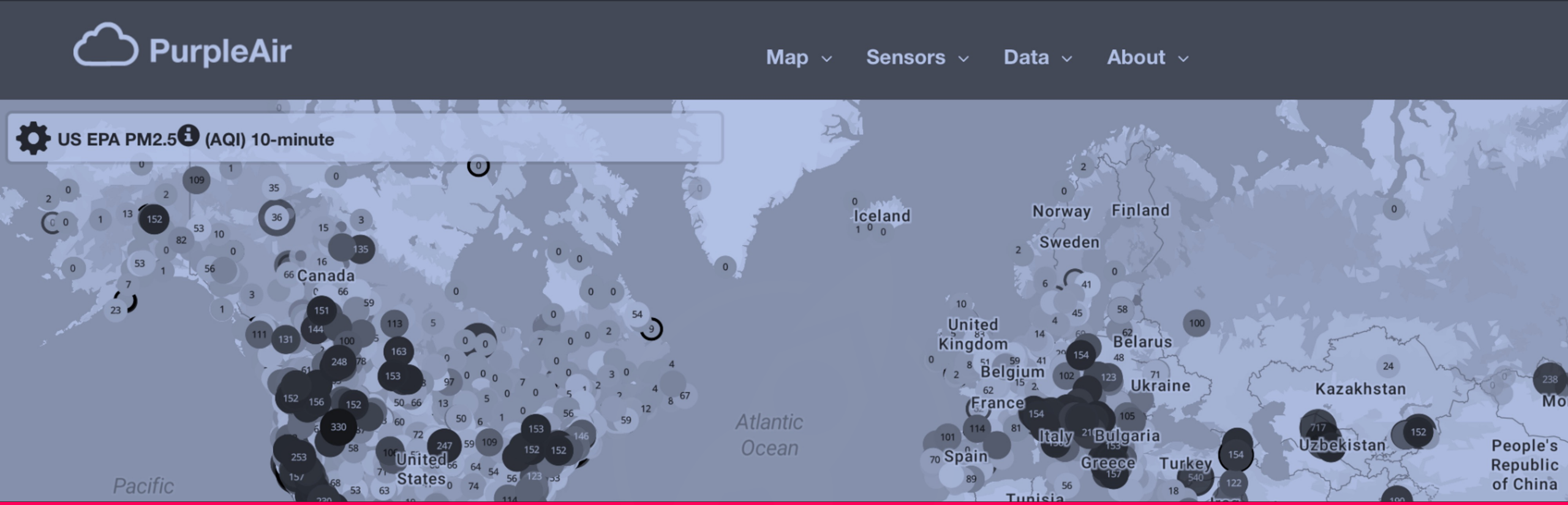
11.5 | DDOS ATTACKS REACHED RECORDS IN 2025 EXCEEDING TERABITS PER SECOND.

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

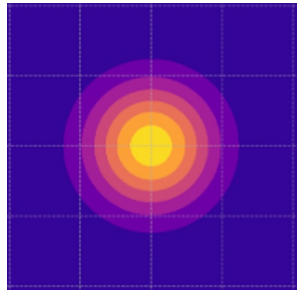
Poor air quality from heat waste and imprecise machine design impacts neural functions

How air pollution alters brain development: the role of neuroinflammation, 2016
The Effect of Noise Exposure on Cognitive Performance and Brain Activity Patterns Biol Psychiatry

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:** $E = kBTln(p)$
- **Section 2.2.4:** $E = kBTln(p)$, $dm/dt = P/c^2$
- **Section 3.4:** $ISM = R_control \times dP_min / N / (dP/dt)$, $\Lambda = 0.24567$
- **Section 3.5:** $ISM = R_control \times dP_min / N / (dP/dt)$, $H(X) = -\Sigma P(x) \times \log_2(P(x))$
- **Section 3.6:** $ISM = R_control \times dP_min / N / (dP/dt)$, $H(X) = -\Sigma P(x) \times \log_2(P(x))$, $dm/dt = P/c^2$
- **Section 3.8:** $dm/dt = P/c^2$, $m(T) = kBTln(2)/c^2$
- **Section 3.10:** $AF = \exp[(Ea/kB) \times (1/T1 - 1/T2)]$
- **Section 3.12:** $dm/dt = P/c^2$, $ISM = R_control \times dP_min / N / (dP/dt)$
- **Section 3.13:** $\Lambda = 0.24567$, $E = kBTln(p)$
- **Section 3.13.2:** $\Lambda = 0.24567$, $E = kBTln(2)$, $AF = \exp[(Ea/kB) \times (1/T1 - 1/T2)]$



Proposal

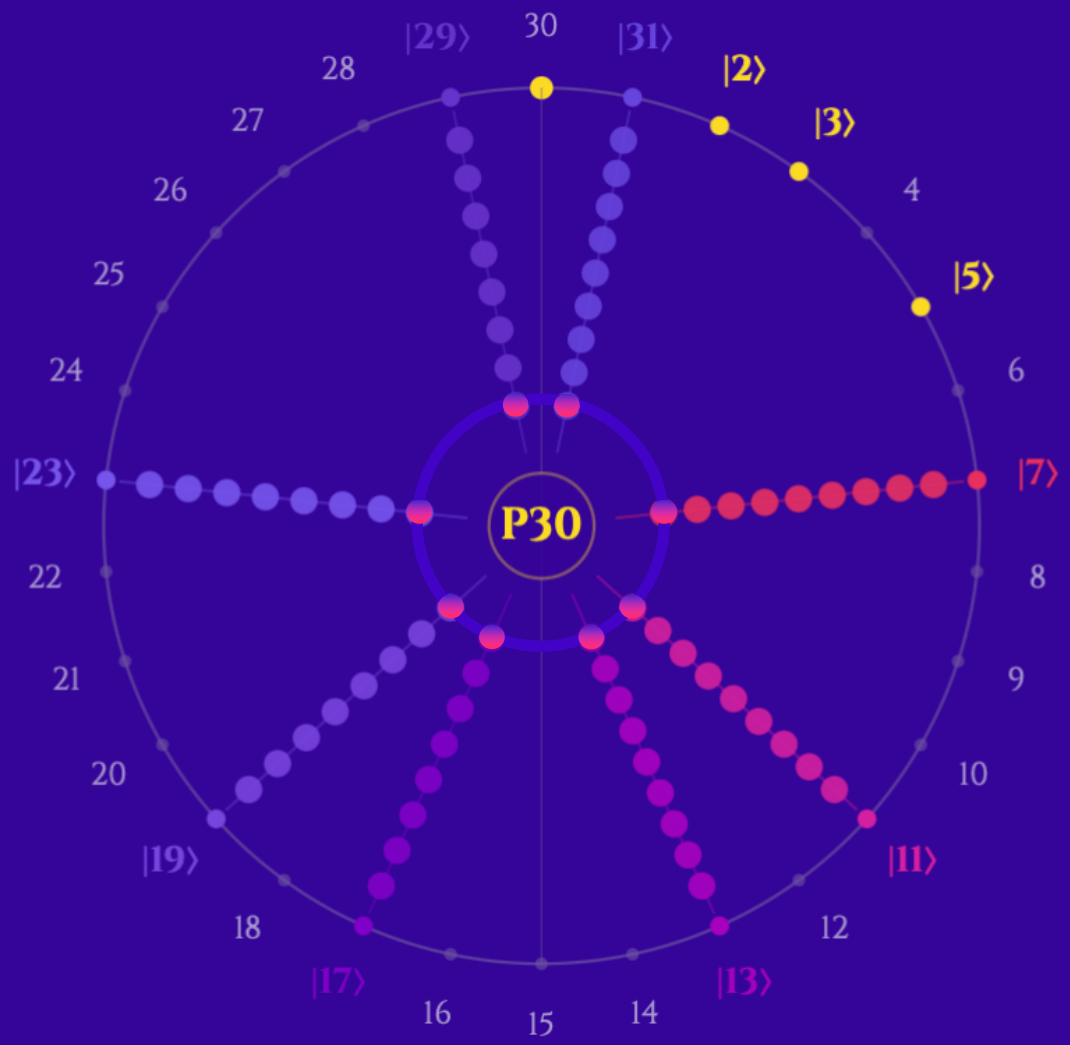
It is proposed to explore data architecture improvements which meet the following product requirements.

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 φ (p), p = 30 matches all 3 requirements. An example architecture is provided which functions with $m(T) = kBT\ln(p)/c^2$. **Infoton 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

SINGLE WORD · ONE BIT | FULL TWEET

COMPLETE

WORD 21 / 21

"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	0	1	1	1	0	1	0	0
BYTE 1 → Y	0	1	1	1	1	0	0	1
BYTE 2 → .	0	0	1	0	1	1	1	0
BYTE 3 → ␣	0	0	1	0	0	0	0	0
BYTE 4 → ␣	0	0	1	0	0	0	0	0
BYTE 5 → ␣	0	0	1	0	0	0	0	0
BYTE 6 → ␣	0	0	1	0	0	0	0	0
BYTE 7 → ␣	0	0	1	0	0	0	0	0

8 CHECK BITS
Hsiao (72,64)

C0	*watches 26*	1
C1	*watches 26*	0
C2	*watches 26*	0
C3	*watches 26*	1
C4	*watches 26*	0
C5	*watches 26*	1
C6	*watches 26*	0
C7	*watches 26*	1

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 would have finished in 63.

PLAY | STEP | RESET | FLIP A BIT

Speed: DEMO | FAST | TURBO | REAL-ISH

OPERATIONS PERFORMED

Write overhead	2688
Read overhead	9576
Total ECC	**12264**

STORAGE TAX

Data delivered	64 BITS · 8 BYTES
Check bits stored	8 BITS · 1 BYTE
Physically stored	**72 BITS · 9 BYTES**
Space spent on checks	12.5% · 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

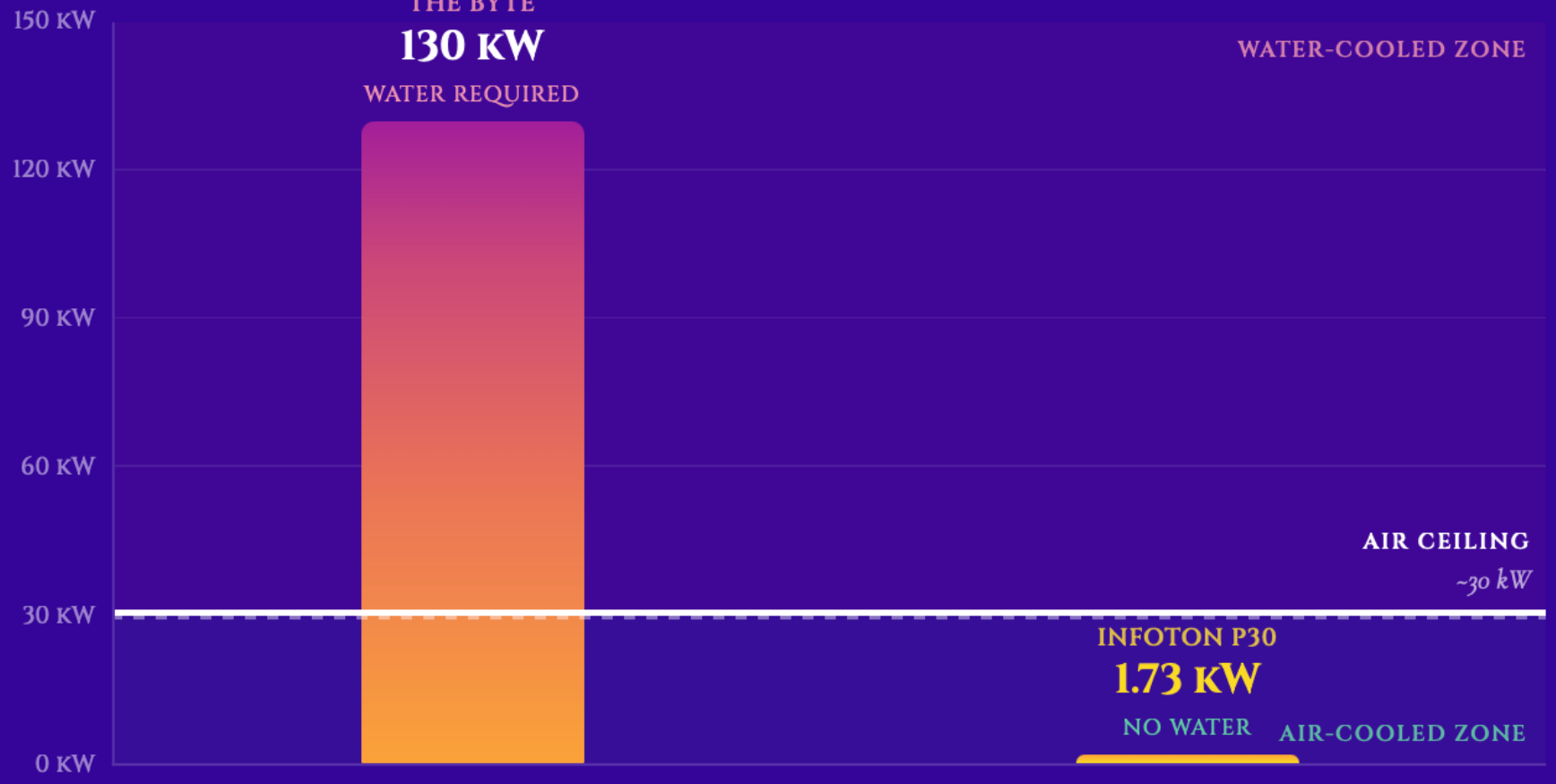
350 K · 77°C (typical DRAM junction)

Per operation	3.349 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

Data centers converted to Infoton P30 — **11,800** 100% of fleet

0 converted — 11,800 converted

FLEET POWER DEMAND

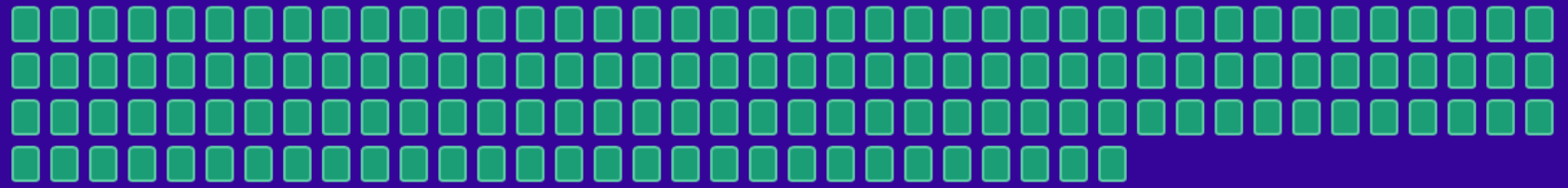
1.8 GW NOW · 43.1 GW REMOVED



byte demand (unconverted) · P30 demand (converted) · demand eliminated

REACTORS AVOIDED (300 MW SMR EACH)

149 AVOIDED



*Each block is one 300 MW reactor proposed for this demand. As the fleet converts, each turns green — avoided outright, its load gone or carried by solar and wind. At full conversion all are green and **zero** remain to be built.*

WASTE HEAT EJECTION STOPPED

43.1 GW



Nearly all electricity into a data center leaves as waste heat. Power saved is heat no longer ejected into air and water.

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

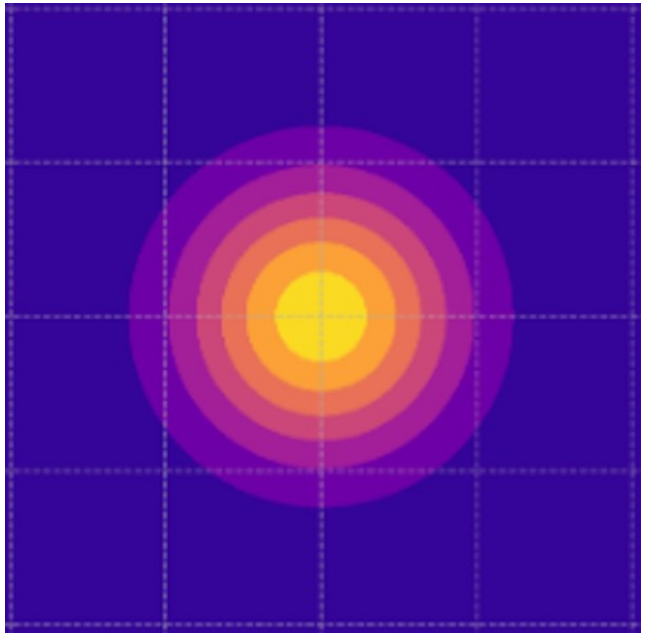
WASTE HEAT STOPPED

HEAT EJECTION ELIMINATED

43.1 GW

thermal, no longer dumped to air and water

Annual waste heat avoided	377 TWh
Equivalent homes\u2019 heating	33.9 M
Water warmable by 1\u00b0C	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, as well as cybersecurity for blockchain and global digital assets.

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**.

