Temporal Asymmetry in Censorship Systems

James Beck
Independent Researcher

Abstract

Deep Packet Inspection (DPI) circumvention is typically understood as a collection of protocol-specific tricks: packet fragmentation, header obfuscation, traffic camouflage. We demonstrate that these tactics are instances of a unified control-theoretic framework in which the attacker manipulates the defender's decision latency until enforcement collapses under its own timing assumptions. We formalize DPI enforcement as a resource-bounded adversarial system with two clocks—transport (when bytes arrive) and inspection (when decisions can be made)—and derive conditions under which the temporal gap enables bypass. We identify three attack families: Δt inflation (pushing evidence past inspection windows), Δt desynchronization (breaking phase alignment), and Δt escalation control (preserving optionality). From these primitives, we derive the Universal Bypass Inequality, a formal condition under which censorship cannot succeed without exceeding computational, temporal, or political budgets. We demonstrate how Encrypted ClientHello (ECH) represents a phase transition from timing manipulation to evidence denial, forcing censors from precision targeting to crude infrastructure bans. This framework generalizes beyond network censorship to any system where commitment outruns grounding: institutional governance, LLM epistemic control, and distributed decision-making under resource constraints.

Keywords: Deep Packet Inspection, censorship circumvention, control theory, temporal dynamics, resource-bounded adversarial systems, ECH, QUIC

---

1. Introduction

Deep Packet Inspection (DPI) systems enforce policy by examining packet contents at network middleboxes. Circumvention techniques—ClientHello fragmentation [1], protocol obfuscation [2], domain fronting [3]—are typically presented as isolated tricks exploiting specific implementation weaknesses. We argue this framing obscures a deeper structure: **DPI bypass is fundamentally about manipulating an adversary's decision latency**.

Every enforcement system operates under temporal and computational constraints. DPI middleboxes must parse, classify, and act on traffic within bounded windows—determined by line rate, buffer depth, and throughput requirements. Bypass techniques succeed not by hiding content, but by ensuring the enforcer cannot obtain decisive evidence and act on it before the protected communication completes.

This insight suggests a control-theoretic model where: - The **transport clock** governs when bytes physically arrive
- The **inspection clock** governs when semantic decisions can be made
- **Bypass occurs when these clocks become sufficiently desynchronized**

We formalize this model, derive necessary and sufficient conditions for bypass, and demonstrate how modern protocols (QUIC, ECH) exploit these conditions systematically rather than accidentally.

1.1 Contributions

1. **Two-clock enforcement model**: Formalize DPI as resource-bounded adversarial control with explicit temporal constraints
2. **Three Δt attack families**: Classify all known bypass tactics as manipulation of decision latency
3. **Universal Bypass Inequality**: Derive formal condition for successful circumvention
4. **ECH as phase transition**: Show how evidence denial forces regime change from precision to crude enforcement
5. **Broader implications**: Demonstrate applicability to institutional failures, LLM governance, any bounded-decision system

1.2 Scope and Limitations

This is a **systems paper**, not an operational guide. We deliberately avoid: - Specific implementation details that enable circumvention - Operational security considerations for deployment - Techniques that could aid adversarial use

We focus on the **control-theoretic structure** that unifies disparate bypass tactics and explains why certain protocols (ECH, QUIC) represent architectural advantages rather than incremental improvements.

---

2. The Two-Clock Model

2.1 Problem Setting

Consider a client attempting to establish a connection to a server through an adversarial middlebox (the "censor"). The censor's goal is to **block** connections to prohibited destinations. The client's goal is to **complete** the connection before blocking occurs.

Two temporal processes govern this interaction:

Transport Clock (T_transport): The physical timing of packet arrival, determined by: - Network latency - Packet segmentation - Retransmission delays - Protocol handshake requirements

Inspection Clock (T_inspect): The semantic timing of decision-making, determined by: - Parsing depth required - Pattern matching complexity - State reconstruction overhead - Classification confidence thresholds

Key Insight: Most DPI implementations assume these clocks are "close enough" that semantic classification can occur within the transport window. Bypass techniques exploit violations of this assumption.

2.2 Enforcement Stage Formalization

We model a DPI enforcement stage j as a tuple:

(W_j, D_j, B_j, C_j)

Where:

W_j(λ): Inspection window - maximum time stage j will wait for evidence before defaulting. Depends on: - Line rate (λ = packets/second) - Buffer capacity - Timeout policies

D_j: Parse depth - amount of state the stage can maintain: - Flow table entries - Partial TLS records - Reassembly buffers

B_j(λ): Decision budget - computational resources per flow: - CPU cycles per packet - Regex/ML inference depth - Heuristic evaluation passes

C_j ∈ {fail-open, fail-closed}: Commitment polarity - what happens under uncertainty: - **Fail-open**: Allow when uncertain (benign default) - **Fail-closed**: Block when uncertain (paranoid default)

κ_j: Political budget - maximum tolerable collateral cost: - K_j(policy) ≤ κ_j where K_j measures false positives, service disruption, legitimacy loss - Tight coupling (low W_j, B_j) increases precision but raises false positive rate under Δt attacks - Loose coupling (high W_j, B_j) reduces precision but increases collateral from crude enforcement

These parameters are **rarely documented** but can be inferred from: - Observed throughput degradation under load - Blocking behavior for ambiguous traffic - Timeout patterns for slow handshakes

2.3 Evidence Accumulation

Let **E(t)** be the evidence available at time t for classifying a flow. For TLS blocking, this might include: - SNI (Server Name Indication) - ALPN (Application-Layer Protocol Negotiation)
- Certificate signatures - Record boundaries and sizes

A DPI stage succeeds in blocking if:

$\exists\, t \le W_j : Score_j(E(t)) \ge \theta_j$

Where Score_j is the classification confidence and θ_j is the threshold for action.

The client's bypass goal is to ensure:

$\forall\, t \le W_j : Score_j(E(t)) < \theta_j$

AND

$T_{handshake} < U$

Where U is the client's patience (timeout threshold).

---

3. Three Δt Attack Families

We identify three fundamental ways to manipulate the relationship between transport and inspection clocks.

3.1 Family A: Δt Inflation

Mechanism: Increase the time until decisive evidence exists in assembled form.

Effect: Push T_E (time to evidence) beyond W_j (inspection window)

Tactics: - **Packet fragmentation**: Split ClientHello across multiple TCP segments or TLS records - **Deliberate jitter**: Introduce timing delays between fragments - **Out-of-order delivery**: Force reassembly overhead

Example: NoDPI

NoDPI [4] fragments the TLS ClientHello such that: - SNI field is split across record boundaries - Fragments arrive with controlled jitter - Reassembly requires maintaining partial state

Under load, DPI boxes with shallow buffers (D_j) or tight windows (W_j) will: - Drop partial records to reclaim memory - Time out waiting for complete evidence - Pass the connection through (if fail-open) or block generically (if fail-closed)

Formal condition:

Let L be a traffic shaping function. Then:

$T_E(L) > W_j(\lambda)$

Implies the DPI stage cannot accumulate enough evidence before its window expires.

3.2 Family B: Δt Desynchronization

Mechanism: Break phase alignment between transport timing and inspection expectations.

Effect: Violate ordering invariants the classifier relies on

Tactics: - **TCP segmentation vs. DPI parsing**: Exploit mismatches between TCP boundaries and TLS record boundaries - **QUIC timing manipulation**: Use 0-RTT, stateless retry, or first-packet behavior to confuse flow tracking - **Proxy chains**: Introduce jitter that desynchronizes correlation heuristics

Example: QUIC vs. TCP

TCP provides the censor **time before evidence**: - 3-way handshake before encrypted payload - Sequential segment assembly - Predictable record boundaries

QUIC provides **evidence immediately but denies time**: - ClientHello in first packet - No separate handshake phase - Connectionless retries

This flips the game from "Can you parse in time?" to "Can you afford to decide instantly?"

QUIC's **Stateless Retry** weaponizes this: - Forces early commitment before connection is authenticated - Makes fail-closed censorship trigger on legitimate retry packets (high false positive cost)

Formal condition:

Let Φ_j be the expected phase relationship between transport and semantic layers.

$\varphi_{observed} \notin \Phi_j$

Implies the classifier's ordering assumptions are violated.

3.3 Family C: Δt Escalation Control

Mechanism: Preserve optionality by deferring high-commitment actions.

Effect: Maintain multiple viable futures until forced to collapse

Tactics: - **Layered defenses**: Start with subtle perturbations, escalate only if needed - **Graceful degradation**: Each layer fails softly to next layer - **Commitment deferral**: Avoid VPN/Tor unless lower layers blocked

Strategic principle:

Early layers (ClientHello fragmentation, QUIC) are: - Low cost - Low visibility - Non-committal (can abort/retry)

Later layers (full tunnels, Tor) are: - High cost - High visibility (announce intent to every policy box) - Committal (difficult to walk back)

Offense in depth is not redundancy for reliability—it's **temporal option preservation** under adversarial observation.

Formal condition:

Let **Comm(L_i)** be the commitment signal (detectability × irreversibility) of layer i.

An optimal strategy minimizes:

$\Sigma\ \mathbf{Comm(L\_i)} \times \mathbf{P(need\_L\_i)}$

Subject to achieving bypass.

---

4. The Universal Bypass Inequality

Synthesizing the three families, we derive a necessary and sufficient condition for successful bypass.

Theorem 1 (Universal Bypass Inequality):

A bypass exists if and only if there exists a traffic shaping function L such that (necessary and sufficient **with respect to the model defined in §2**):

$$(\mathbf{T\_E(L) > W\_j(\lambda)} \lor \mathbf{Cost(f(E)) > B\_j(\lambda)} \lor \mathbf{E(t) = \emptyset})$$

$$\land\ \mathbf{T\_E(L) + A\_j \geq T\_app\text{-}commit}$$

$$\land\ \mathbf{T\_handshake(L) < U}$$

Where: - **T_E(L)**: Time until decisive evidence exists under shaping L - **W_j(λ)**: Inspection window under load λ - **Cost(f(E))**: Computational cost to classify evidence E - **B_j(λ)**: Per-flow budget under load λ - **E(t)**: Evidence available at time t (∅ if encrypted/unavailable) - **A_j**: Action latency (time to inject RST, redirect, block) - **T_app-commit**: When application-layer commitment occurs - **U**: Client patience threshold - **T_handshake(L)**: Total handshake time under shaping L

Interpretation:

The censor fails if: 1. **Evidence arrives too late** (T_E > W_j) 2. **Classification costs too much** (Cost > B_j) 3. **Evidence doesn't exist** (E = ∅)

AND blocking action arrives after commitment **AND** handshake completes before client timeout.

Proof sketch:

(1) If evidence arrives after the inspection window, the stage must commit without full information. Under fail-open policy, this allows bypass. Under fail-closed, this causes false positives, creating political cost.

(2) If classification exceeds per-flow budget under load, the stage must either drop flows (reducing legitimacy) or reduce inspection depth (enabling bypass).

(3) If evidence is cryptographically unavailable (E = ∅), no parsing budget helps. The censor must resort to IP/protocol bans (crude enforcement).

(4) If A_j + T_E ≥ T_app-commit, blocking occurs after the application has already established state, reducing effectiveness.

(5) If T_handshake ≥ U, the client abandons the attempt, achieving the censor's goal by attrition. ■

Corollary 1: All known DPI bypass tactics are instances of manipulating one or more terms in the UBI.

Corollary 2: As censors harden one term (e.g., increase W_j), they create pressure on others (e.g., increase false positives, reduce throughput, increase operational cost).

---

5. Case Studies

5.1 NoDPI: Pure Δt Inflation

Mechanism: Fragment TLS ClientHello across records with controlled jitter

UBI term exploited: T_E > W_j

Effectiveness: - High against shallow-buffer DPI (consumer ISPs) - Low against deep-stateful inspection (national firewalls) - Zero privacy protection (IPs visible, no encryption beyond TLS)

Countermeasures: - Increase buffer depth D_j (expensive in hardware) - Extend window W_j (reduces throughput) - Fingerprint fragmentation patterns (cat-and-mouse)

Strategic role: Layer 1 in escalation ladder—cheap, low-visibility, fails softly.

5.2 QUIC: Commitment Polarity Probe

Mechanism: First-packet ClientHello + stateless retry forces early decisions

UBI term exploited: Forces C_j visibility (fail-open vs. fail-closed)

Key insight: QUIC doesn't hide evidence—it **forces the censor to reveal policy** immediately.

Important caveat: QUIC's effectiveness is **deployment-specific** and depends on censor policy. It is not inherently a bypass technique but rather a **diagnostic tool** that reveals enforcement behavior.

Stateless Retry specifically: - Legitimate QUIC feature (RFC 9000) - Requires censor to either: - Allow (fail-open) ⟶ bypass succeeds - Block all retry packets (fail-closed) ⟶ breaks legitimate QUIC, high cost

Effectiveness: - **Not** a bypass technique per se - A **diagnostic tool** revealing C_j - Informs choice of subsequent layers

QUIC as Δt weapon: - TCP: Evidence accumulates slowly, censor has time to decide - QUIC: Evidence arrives immediately, censor must commit instantly under load

5.3 ECH: Evidence Denial (E(t) = ∅)

Mechanism: Encrypt ClientHello, making SNI/ALPN unavailable

UBI term exploited: E(t) = ∅ (evidence never arrives)

Phase transition:

Pre-ECH: - Censor optimizes: parsing speed, state depth, decision latency - Attacker fights over: T_E, W_j, B_j, A_j

Post-ECH: - Censor loses targeted blocking capability - Must escalate to: DNS blocking, IP blocking, protocol bans

This is regime change, not incremental improvement.

ECH doesn't make censorship slower—it makes it cruder.

Three-layer ECH bypass model:

Layer 0: DNS/Key Acquisition - Requires DoH (DNS-over-HTTPS) or DoT (DNS-over-TLS) - **Vulnerability:** Censor can block DoH resolvers - **Tactic:** Domain fronting for DoH connection, boutique resolvers

Layer 1: ECH Handshake - ClientHelloOuter (visible, decoy) + ClientHelloInner (encrypted) - **Vulnerability:** Fingerprinting via size distribution - **Tactic:** Padding strategies, decoy randomization

Layer 2: Fallback Discipline - Client MUST NOT downgrade to cleartext if ECH fails - **Fail-closed client:** Connection dies if ECH blocked (secure but annoying) - **Fail-open client:** Falls back to cleartext (defeats purpose)

Strategic conclusion:

ECH forces the censor to abandon "Smart Cop" (DPI, parsing, logic) and become "Dumb Cop" (IP bans, port bans, protocol bans).

Dumb Cop tactics are: - **Expensive** (collateral damage) - **Rigid** (can't adapt to evasion) - **Politically costly** (visible, blunt)

Formal model under ECH:

Since E(t) = ∅, the UBI collapses to:

(T_E = ∞) ∧ (T_handshake < U)

The censor can only win by: - **Preventing key acquisition** (block DoH) - **IP blocking** (collateral damage) - **Protocol ban** (block ECH extension ID globally)

All of these are **policy decisions**, not technical wins.

---

6. Regime Transitions and Escalation Ladders

6.1 The Enforcement Regime Ladder

As bypass techniques mature, enforcement escalates through predictable regimes:

Regime 1: Content-Based DPI - Inspect packet contents, classify semantically - **Requires:** T_E < W_j and Cost(f(E)) < B_j - **Defeated by:** Δt inflation, encryption

Regime 2: Behavioral Heuristics - Classify based on timing, sizes, patterns - **Requires:** Statistical models, ML classifiers - **Defeated by:** Δt desynchronization, traffic shaping

Regime 3: Protocol Bans - Block entire protocols/extensions (QUIC, ECH) - **Requires:** Policy decision (collateral damage acceptable) - **Defeated by:** Protocol obfuscation, mimicry

Regime 4: Infrastructure Bans - Block IPs, ASNs, resolver services - **Requires:** Willingness to break legitimate services - **Defeated by:** Distributed infrastructure, CDN fronting

Key observation: Each escalation **increases cost and decreases precision**.

The censor's dilemma: precision requires DPI (defeated by Δt), but abandoning DPI requires crude enforcement (politically expensive).

6.2 The Offense-in-Depth Ladder

Optimal bypass strategy mirrors the regime ladder:

Layer 0: Normal TLS, do nothing (baseline)

Layer 1: Dumb DPI confusion (ClientHello fragmentation, packet jitter) - Cost: ~5ms added latency - Visibility: Low (looks like network jitter) - Commitment: None (fails gracefully)

Layer 2: Protocol variance (QUIC, alt ports, ECH) - Cost: ~20ms for ECH key fetch - Visibility: Medium (announces protocol intent) - Commitment: Low (can retry without)

Layer 3: Encrypted tunnels with camouflage (obfsproxy, shadowsocks) - Cost: ~100ms tunnel setup - Visibility: High (persistent tunnel connection) - Commitment: Medium (leaves server-side trace)

Layer 4: Full anonymization (Tor, I2P) - Cost: ~500ms multi-hop latency - Visibility: Maximum (announces adversarial intent) - Commitment: High (joins observable set)

Strategic principle: Start subtle, escalate only when forced.

---

7. Broader Implications

The Δt bypass framework generalizes to any system where **commitment outruns grounding**. We do not claim empirical equivalence across these domains, only structural equivalence of the control problem: bounded decision-making under temporal asymmetry.

7.1 Institutional Governance

Organizations fail when decision-making (fast) outpaces evidence accumulation (slow). While institutional governance operates at different scales and under different constraints than network censorship, the systems share structural similarities in their control dynamics.

Structural parallels to DPI: - **W_j**: How long leadership waits for analysis before deciding - **B_j**: Resources allocated to due diligence per decision - **T_E**: Time required for rigorous evaluation - **C_j**: Fail-open (permissive) vs. fail-closed (paranoid) culture

Bypass analogue: Rushed decisions under pressure create vulnerability to: - Narrative capture (selective evidence) - Momentum exploitation (commit before questioning) - Option exhaustion (force early commitment)

7.2 LLM Epistemic Control

Language models exhibit temporal incoherence when **linguistic fluency (fast) outruns grounding (slow)**. This paper does not claim a complete equivalence between network censorship and LLM governance, only that they share a common control structure where commitment outruns verification.

Structural parallels to DPI: - **W_j**: Context window / inference budget - **T_E**: Time to verify claims against sources - **E(t)**: Evidence actually constraining output - **C_j**: Whether system blocks on uncertainty

Bypass analogue: Hallucinations occur when: - Output is generated faster than grounding can verify - Confidence accumulates without evidence - Contradictions pass inspection window undetected

Solution (Epistemic Governor): Architectural separation where: - Language proposes (fast) - Evidence commits (slow) - No closure without verification

Same control structure as censorship circumvention, inverted: **slow the commit, not the evidence**.

7.3 Distributed Consensus

Byzantine fault tolerance protocols face similar constraints: - **W_j**: Round timeout - **T_E**: Time for majority quorum - **B_j**: Verification cost per message - **A_j**: Action latency to finalize

Adversaries exploit timing to: - Delay evidence past commit window (T_E > W_j) - Exhaust verification budget (Cost > B_j) - Force premature consensus (commit before quorum)

---

8. Discussion

8.1 Why This Framework Matters

Unifies disparate tactics: Shows ClientHello fragmentation, QUIC behavior, and ECH are instances of the same control problem, not unrelated tricks.

Predicts effectiveness: The UBI provides formal conditions for when tactics work vs. fail.

Reveals fundamental trade-off: Censors face a precision-robustness curve: - **Precision** (targeted blocking) requires tight coupling between transport and inspection clocks → vulnerable to Δt attacks - **Robustness** (surviving Δt manipulation) requires looser coupling → increases collateral damage (high false positive rate or crude infrastructure bans)

This explains regime transitions: censors move along the feasible frontier from DPI (precise, brittle) toward protocol/infrastructure bans (robust, crude) as bypass techniques mature.

Explains regime transitions: Shows why ECH represents phase change (evidence denial) rather than incremental improvement.

Generalizes beyond networking: Demonstrates applicability to institutional failures, LLM control, distributed systems.

8.2 Limitations

No operational guidance: We deliberately avoid implementation details that would enable adversarial use.

Simplified model: Real DPI systems have ML classifiers, adaptive heuristics, and political constraints not captured by the UBI.

No empirical validation: We present formal framework, not measurements of production systems.

Ethical constraints: We do not discuss techniques that would aid authoritarian censorship.

8.3 Future Work

Empirical measurement: Instrumentation to infer (W_j, B_j, C_j, κ_j) from observable behavior.

Adaptive models: Extend UBI to adaptive parameters W_j(λ,t), B_j(λ,t) with hysteresis and update costs; analyze as repeated resource-bounded game. This would capture censor learning and protocol evolution dynamics.

Multi-stage cascades: Model censorship as series of stages, not single middlebox.

Political cost functions: Formalize collateral damage as economic constraint.

Cross-domain applications: Develop UBI variants for institutional governance, LLM control.

---

9. Conclusion

We have shown that DPI circumvention is best understood not as protocol exploitation, but as **manipulation of an adversary's decision latency**. The Universal Bypass Inequality formalizes conditions under which enforcement collapses under its own timing assumptions. All known bypass tactics—fragmentation, protocol variance, encryption—are instances of forcing $(T_E > W_j) \vee (Cost > B_j) \vee (E = \emptyset)$.

ECH represents a phase transition: not making censorship slower, but making it cruder. By removing semantic evidence entirely ($E = \emptyset$), ECH forces censors from precision targeting to infrastructure bans, fundamentally changing the economics and politics of control.

This framework generalizes to any system where fast commitment outruns slow grounding: institutions, language models, distributed consensus. The same control-theoretic structure explains why organizations make rushed decisions, why LLMs hallucinate confidently, and why Byzantine protocols fail under timing attacks.

The invariant: Systems that lack architectural separation between proposal and commitment will fail when observation cannot keep pace with action.

Censorship circumvention, properly understood, is a special case of this universal dynamic.

References

[1] NoDPI Project. "Deep Packet Inspection Circumvention Utility." GitHub, 2024.

[2] Dingledine, R., Mathewson, N., & Syverson, P. "Tor: The Second-Generation Onion Router." USENIX Security, 2004.

[3] Fifield, D., et al. "Blocking-Resistant Communication through Domain Fronting." PETS, 2015.

[4] Winter, P., et al. "How the Great Firewall of China is Blocking Tor." FOCI, 2012.

[5] Rescorla, E., et al. "The Transport Layer Security (TLS) Protocol Version 1.3." RFC 8446, 2018.

[6] Iyengar, J., & Thomson, M. "QUIC: A UDP-Based Multiplexed and Secure Transport." RFC 9000, 2021.

[7] Rescorla, E., et al. "TLS Encrypted Client Hello." Internet-Draft, 2024.

[8] Sherry, J., et al. "Making Middleboxes Someone Else's Problem: Network Processing as a Cloud Service." ACM SIGCOMM, 2012.

[9] Anderson, T., et al. "On the Scalability of Data Center Networks." ACM SIGCOMM Computer Communication Review, 2010.

[10] Dusi, M., et al. "Traffic Classification Through Simple Statistical Fingerprinting." ACM SIGCOMM Computer Communication Review, 2007.

[11] Beck, J. "The Coherence Criterion: A Unified Framework for Stability in Hierarchical Systems." Zenodo, 2025. DOI: 10.5281/zenodo.17726790.

[12] Ashby, W.R. "An Introduction to Cybernetics." Chapman & Hall, 1956.

[13] Khanafer, A., et al. "Stability of Congested Networks under Multipath Routing." IEEE Trans. Automatic Control, 2009.

Appendix A: Formal Definitions

Definition A.1 (Traffic Shaping Function): A traffic shaping function $L : \text{Packet Stream} \to \text{Packet Stream}$ modifies timing, segmentation, or ordering while preserving semantic content.

Definition A.2 (Evidence Function): E(t) : Time ⟶ Evidence is the set of packet features available for classification at time t.

Definition A.3 (Classifier Score): Score_j(E) : Evidence ⟶ [0,1] maps evidence to classification confidence.

Definition A.4 (Inspection Window): W_j(λ) is the maximum time stage j will buffer packets before committing, as a function of packet arrival rate λ.

Definition A.5 (Commitment Polarity): C_j ∈ {fail-open, fail-closed} determines default action under uncertainty.

Definition A.6 (Action Latency): A_j is the time required to inject blocking packets (RST, redirect) after decision.

Appendix B: UBI Derivation Details

We omit the full queueing-theoretic derivation here; the inequality follows directly from bounded-buffer and bounded-service-time assumptions common to DPI architectures. A complete formalization would model DPI stages as M/G/1 queues with finite buffers and show that under load λ, waiting time exceeds W_j with nonzero probability, forcing early commitment when classifier service time exceeds B_j.

Acknowledgments: This work emerged from collaborative formalization sessions across multiple AI systems, demonstrating the value of multi-model semantic amplification for theoretical development. All errors remain the author's responsibility.

Conflict of Interest: The author has no financial interests in circumvention technologies or censorship systems.

Ethical Statement: This research is presented for academic understanding of control-theoretic properties of adversarial systems. The author does not condone circumvention of legitimate security policies or authoritarian use of censorship technologies.