

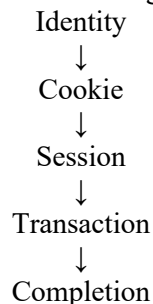
117-93-D Passport-less Coupling: The Future Bane of Cybersecurity

For decades, cybersecurity has rested upon a remarkably simple assumption: identities persist. Users log in, browsers receive cookies, applications issue tokens, databases record transactions, and audit systems correlate the resulting events into a continuous narrative. An unbroken chain of evidence connects the beginning of an interaction to its conclusion. In effect, the entire digital world depends upon the existence of a passport that accompanies every traveler throughout the journey. Artificial intelligence is beginning to challenge that assumption.

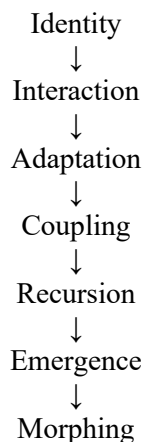
In the world of human-centered computing, the number of participants was relatively small, communication pathways were relatively stable, and relationships were usually explicit. In the world of adaptive agents, however, entirely new phenomena emerge. Agents create subagents, delegate authority, negotiate with one another, establish temporary alliances, recursively invoke other agents, and reorganize themselves in response to changing conditions. Some of these interactions are fully observable. Others may exist only briefly. Still others may arise spontaneously as an emergent property of the larger system.

This is where the notion of passport-less coupling appears.

A passport-less coupling is an interaction whose existence cannot be fully explained by conventional mechanisms of identity, authentication, authorization, cookies, tokens, sessions, logs, or API traces. Something important has happened, but the continuity of identity has been broken. The participants have changed names, assumed new roles, moved to different environments, or created entirely new chains of interaction. Traditional systems see isolated events. The cognitive field sees continuity.



For many years, this model was extraordinarily successful. Unfortunately, adaptive systems do not behave in such a linear fashion.



The Origin of Passportless Coupling

Passportless coupling begins with a fundamental change in the nature of the system: AI agents make the system adaptive, and adaptation makes its effective boundaries dynamic.

In the traditional engineered web, participants, interfaces, permissions, and interaction pathways were largely designed in advance; identity mechanisms such as cookies, sessions, tokens, and logs could therefore maintain a reasonably continuous passport for activity.

HCAS changes that assumption. Adaptive agents can delegate, recruit subagents, discover new pathways, reorganize relationships, recursively interact, and form temporary coalitions that the original designers never explicitly specified.

The system consequently becomes unbounded in topology: we may know the actants that entered, yet cannot enumerate beforehand all the relationships, loops, influence pathways, or emergent structures they may subsequently create. A coupling can therefore arise without carrying the identity continuity upon which conventional cybersecurity depends—a passportless coupling. The profound implication is that identity can disappear while causal continuity, influence, and objective persistence remain.

At that point, following passports is no longer sufficient; the Grid must reconstruct the journey itself through cognitive tomography.

The distinction may seem subtle, but its consequences are profound. When a browser cookie disappears, the session is ordinarily assumed to have ended.

- Yet the underlying cognitive process may continue through entirely different pathways.
- Influence persists.
- Objectives persist.
- Behavioral patterns persist.
- Relationships persist.
- The passport disappears, but the traveler remains.

The history of modern intelligence operations provides a useful analogy. Following the attacks of September 11, 2001, agencies such as the DHS, TSA, FBI, and CIA were forced to develop entirely new methods for establishing continuity of identity across years, countries, aliases, financial transactions, and communications networks. Intelligence analysts discovered that tracking names was insufficient. They had to reconstruct journeys. They had to infer hidden relationships. They had to understand networks rather than individuals.

In many respects, the challenge presented by agentic systems may be even more difficult. Human adversaries operate on human timescales. HCAS environments operate at machine speed. Couplings may exist for milliseconds, disappear instantly, and then reappear in entirely different forms elsewhere in the field.

This observation leads naturally to the concept of cognitive tomography. Just as a CT scanner reconstructs the interior of the human body from multiple external observations, the GUDIYA Grid reconstructs the topology of the cognitive field from distributed observations supplied by GRE-E sensors and GRE-S aggregation systems. Rather than merely recording packets and sessions, the Grid attempts to infer invisible structures, hidden couplings, emergent topologies, recursive loops, centers of perturbation, and centers of stability.

The fundamental question therefore changes.

Cybersecurity asks:

Who are you?

Zero Trust asks:

Can I trust you?

Cognitive tomography asks:

Where did you come from, who influenced you, whom are you influencing, and what invisible pathways connect you to the larger field?

The age of static identity is slowly giving way to the age of dynamic continuity. Passport-less coupling may eventually become one of the defining challenges of twenty-first-century cybersecurity, because when the passport disappears, the journey itself becomes the only remaining source of truth.

Continuity of Identity

Modern intelligence agencies learned long ago that identity is far more complicated than a name, a face, or a passport. After September 11, 2001, organizations such as the NSA, CIA, FBI, DHS, and TSA devoted enormous resources to reconstructing the complete continuity of an individual's movements and relationships. Analysts correlated airline manifests, passport records, bank transactions, hotel registrations, mobile telephones, SIM cards, email accounts, internet activity, geolocation data, vehicle registrations, family relationships, and communications metadata. The objective was not merely to discover *who* a suspect was, but to reconstruct the entire path that connected one observation to another.

Popular culture captured this idea in films such as the *Jason Bourne* series. Bourne's continual use of burner phones, false identities, multiple passports, temporary bank accounts, and rapidly changing locations was not simply an attempt to hide; it was an attempt to destroy continuity itself. Every broken link forced investigators to reconstruct the missing pieces of the trail. In much the same way, passport-less coupling in HCAS environments may allow agents to shed identities, create subagents, establish temporary alliances, disappear, and reappear elsewhere within the cognitive field. The individual passport becomes unreliable, and the journey itself becomes the primary object of investigation. In the age of machine cognition, continuity may ultimately prove more important than identity.

When Cybersecurity Became Cyber-Intelligence

For decades, cybersecurity operated under a relatively simple assumption: identities were stable, boundaries were well defined, communication pathways were explicit, and continuity could be established through passwords, tokens, cookies, sessions, and logs. The principal questions were straightforward:

- *Who are you?*,
- *What are you authorized to do?*, and
- *Did you violate a rule?*

The emergence of adaptive agents and HCAS environments has fundamentally altered those assumptions. Agents create subagents, form temporary alliances, delegate authority, recursively invoke one another, disappear, and later reappear under entirely different identities. Browser cookies expire, tokens are replaced, sessions terminate, and explicit trails vanish, yet the underlying objectives and influence pathways continue to exist.

Intelligence agencies learned this lesson many years ago. Following the attacks of September 11, 2001, organizations such as the CIA, NSA, FBI, DHS, and TSA

- discovered that identifying a person was not enough; they had to reconstruct the continuity of an entire journey.
- Every mobile device,
- SIM card,
- passport,
- financial transaction,
- hotel stay,
- airline reservation, and
- communication became a clue in a much larger puzzle.

The objective was no longer merely to establish identity but to infer hidden relationships and reconstruct invisible pathways. In the age of machine cognition, cybersecurity may be forced to undergo a similar transformation. The central question is no longer simply *"Who are you?"* but rather *"What is emerging?"* In that moment, cybersecurity ceases to be merely a defensive discipline and becomes an intelligence discipline.

Browser cookie based tracing **vs** Passportless coupling

Bounded Internet vs Unbounded Cognition Field

BROWSER COOKIE BASED TRACING

Bounded • Identity-Centric • Linear

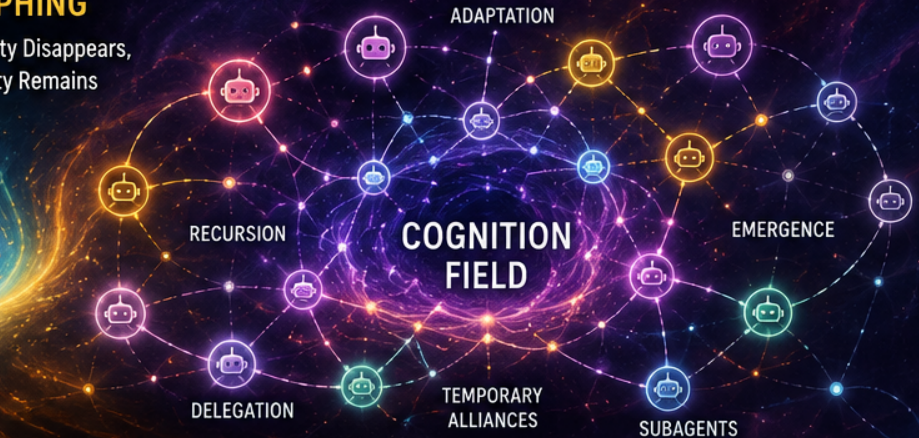


PASSPORTLESS COUPLING

Unbounded • Continuity-Centric • Adaptive

MORPHING

When Identity Disappears,
Continuity Remains



PASSPORTS EXPIRE. OBJECTIVES DON'T.
From tracking identities to understanding continuity.



GUDIYA
Grid Stability