



THE ALGORITHM WAR:

THE WORLD
BENEATH
THE WORLD

By John Threat



Editor's Note: This is the first article in a three-part series. The next article will explore how algorithmic warfare is reshaping institutions, economies, and governance worldwide and some frameworks and systems we can use to dream up a new direction for these technologies.

In September 2025, Benjamin Netanyahu admitted something remarkable on live television: Israel was losing the social media war. Not a military war. Not an economic war. The *algorithm war*.

Leaders from the most powerful nations on earth involved in conflicts aren't mentioning troop movements or the amazing new munitions like drones and robots: they are concerned with the algo war. The war for perception.

The Algorithm war determines geopolitical leverage internationally, and controls morale at home which in turn determines political will. Every major nation state is working to enter this emergent battlefield with new weapons, techniques, intelligence offices and military units. The algo war will shape geopolitical futures for the next 100 years.

Marshall McLuhan (Medium is the Message) quipped: "We don't know who discovered water, but we're pretty sure it wasn't a fish." The same applies to algorithmic infrastructure. We're all swimming in it, shaped by it, but most institutions still can't see it operating. This invisibility is algorithmic warfare's primary advantage – the battlefield is everywhere and nowhere, the weapons are engagement metrics and recommendation systems, and most decision-makers don't even know they're under attack.

From our complex connected world, the algorithm has emerged as a new domain, a substrate in our society to fight over – for hegemony. It may just determine who controls this planet.

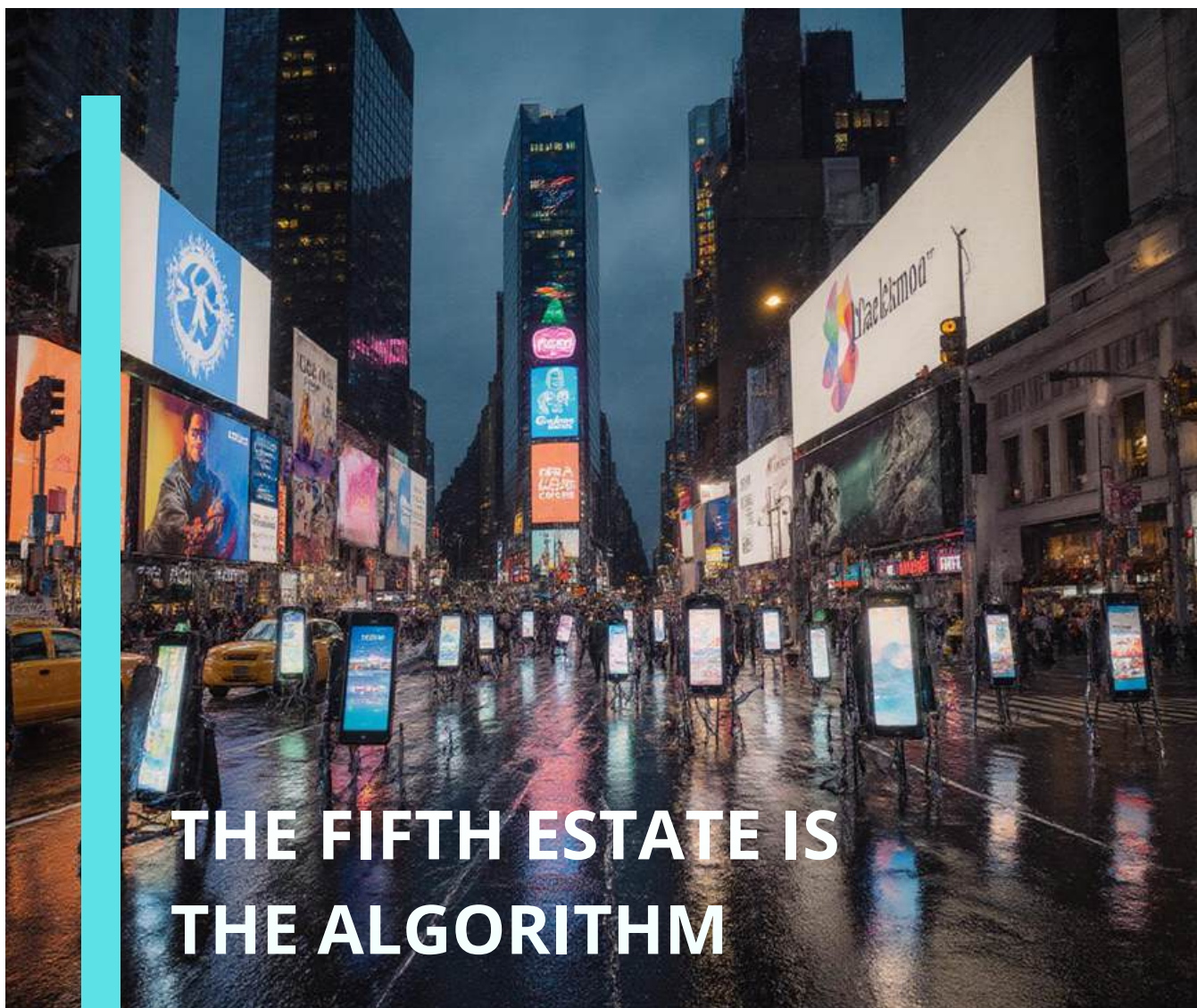
This is the world beneath the world. The unseen war.

THE TIK TOK DOCTRINE

Never have two superpowers publicly battled for control of an algorithm. The multi-year TikTok fight ended in an unprecedented arrangement: shared custody between rivals. The USA didn't want to ban it, they wanted IN on the data so badly they let China keep a slice, as long as they gave America a cut.

Compare this to the last great weapon system that proliferated. The nuclear bomb sparked elaborate games of espionage, sabotage, and resource denial, all behind the scenes over decades. The TikTok battle happened in public, with bipartisan crowds in the streets demanding access to their feeds.

China requires U.S. products to reveal their algorithms in full before market entry into their country. The U.S. does the opposite: algorithms aren't questioned as long as you pay enough to the Congressional lobby apparatus. The algorithm has become a geopolitical lever, its data a global resource.



THE FIFTH ESTATE IS THE ALGORITHM

We have a new mature domain of power. The four estates: leaders, elites, the people, the press have been disrupted. At the turn of the century, some tried to assign the fifth estate to bloggers, but they've simply merged into the fourth. Bloggers are journalists now, and journalists are podcasters. The actual fifth estate is the algorithm: the new power dynamic in geopolitics.

Historical leaders kept wizards and alchemists to navigate foreign affairs; advisors who saw patterns invisible to others. Today, the missing position in most cabinets and institutions isn't the social media manager or CIO (though institutions often confuse the two for this praxis). It's the **Algorithmist**: someone who understands the emergent field now controlling the fate of nation-states, companies, societies and culture.

THE DATA THAT BINDS



This battlefield emerged from tech utopianism. Pitched as the medium for global democracy and understanding, it became one of the most powerful asymmetries since the nuclear bomb. Runaway surveillance capitalism that weaponizes global connectivity itself. A Jevons paradox of data: instead of clarity between nations, confusion. Instead of understanding, manufactured consent at the press of a button.

In Myanmar, Facebook's recommendation engine amplified genocidal content against the Rohingya. UN investigators concluded the platform played a "determining role" in the violence. Not contributing. Determining. [1]

In Ukraine, the information war runs parallel to the kinetic one. The Delta battlefield management system collapsed targeting cycles from 72 hours to 2 minutes; but the war for narrative moves even faster. TikTok targeting drone strikes. Telegram resistance channels. Algorithms deciding which atrocities trend and which disappear, and amplifying for example video game footage of a jet fighter called the Ghost of Kiev that fooled some air force vets, built morale for Ukraine and suppressed that of Russia. The Arab Spring was celebrated as a Twitter revolution.[2]

A decade later, the same platforms that enabled organizing now enable surveillance, manipulation, and suppression. The tools didn't change. The understanding of how to weaponize them did.

[1] Source: Marzuki Darusman, Chair of the UN Independent International Fact-Finding Mission on Myanmar, briefing to the UN Human Rights Council, March 12, 2018. Darusman stated social media had a "determining role" in the conflict, adding "as far as the Myanmar situation is concerned, social media is Facebook, and Facebook is social media." (Reuters, March 12, 2018.)

[2] Source: Philip N. Howard et al., "Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring?" Project on Information Technology and Political Islam, University of Washington, 2011. Plus Clay Shirky, Foreign Affairs, "The Political Power of Social Media," January/February 2011 — the canonical "Twitter revolution" framing.

AI: THE WEAPON FORMED FROM THE ALGORITHM



Everything dangerous about algorithmic warfare is now accelerating exponentially. Every new domain: outer space, underwater, cyber, brings new tools and weaponization. AI is born from the digital realm's infrastructure, literally made from algorithms. It's the perfect weapon for this domain.

Deepfakes that once required specialist teams can now be generated by a teenager with a laptop. Sentiment manipulation that needs vast troll farms can be automated at scale. The friction that once limited propaganda; human labor, production costs, distribution time, has collapsed.

Systems that learn, adapt, and scale faster than any human institution can respond are already online. They've calculated your potential response and challenged it before it becomes policy.

Technology is moving faster than ethics and governance. Open source, corporate extraction, state hegemony, everyone is racing. Even tech-forward institutions lag behind, convening AI ethics conferences while pushing policy for products that have evolved multiple iterations by the time the law passes a year later. And who's implementing anything? This domain hides in the infrastructure of global commerce, governance, and communications, running on mobile nodes that can exist anywhere. Institutions have to adapt by being in front of the change and not chasing it from behind.

DATA COLONIZATION

The superpowers are also exporting the tools for the algo war to extend their hegemony. Data colonization through infrastructure.

The U.S. has Palantir, now embedded in allied nations' intelligence systems, their data flowing back to American servers. China has Mininglamp, selling social credit and predictive policing to countries but the architecture feeds Beijing. Saudi Arabia's HUMAIN: \$100 billion in AI initiative branded as "smart cities," and exported to neighbors. [3]

Venture capital is pouring money into corporate click farms recognizing what first started as hidden cell phone racks in basements in countries most people can't find on a map, that power should be up for sale on the stock market as a SaSS and receive government contracts. [4]

[3] Sources: NYT investigation, Paul Mozur, Muyi Xiao, John Liu, "An Invisible Cage: How China is Policing the Future," June 25, 2022 (Mininglamp / predictive policing architecture feeds Beijing). Atlantic Council, "The West, China, and AI surveillance" (December 2020) — export pattern through Belt and Road. Reuters / Arab News, May 13, 2025 — HUMAIN launched by Saudi Arabia's Public Investment Fund as a \$100B sovereign AI initiative including data centers, the ALLAM Arabic-first LLM, and AI infrastructure for NEOM "cognitive cities," with declared regional export ambition by 2030.

[4] Source: NCRI / Rutgers, "America Last: How Fuentes's Coordinated Raids and Foreign Fake-Speech Networks Inflate His Influence," Network Contagion Research Institute, December 2025 — documents foreign bot-farm amplification of US political discourse, the SaaS-ification of inauthentic engagement, and platform algorithmic interpretation of synthetic engagement as organic legitimacy.

Nations without resources to build their own systems are giving up their data sovereignty, products sold to them as a way to shape their societies by surveillance capitalism. Either way, their data enters another nation's data dark pool, their citizens profiled by someone else's algorithm, their sovereignty quietly captured through the infrastructure they thought they purchased.

Traditional geopolitical frameworks assume sovereignty is defended through borders and military force. Algorithmic infrastructure don't see borders; it flows through them like water through sand. The defensive advantage that defined centuries of warfare has inverted: a well-coordinated campaign using open-source tools costs thousands, while defending against it costs billions.

Switzerland's military formally rejected Palantir after a security audit concluded that U.S. intelligence agencies could access sensitive Swiss defense data through the CLOUD Act – regardless of where servers physically sit. The Swiss report warned that data leaks from Palantir systems “cannot be technically prevented.” For a neutral nation outside NATO, trading sovereignty for efficiency was unacceptable, for now this is an outlier and not a trend.

DATAFASCISM



A consequence of the algorithm war is the decline of democracy globally.

The algorithm is weakening all institutions because they fundamentally don't currently have the ability to understand or respond to the algorithm. The internet was supposed to bring openness. Instead, countries are scrambling to maintain digital sovereignty through firewalls while surveillance capitalism hands governments the tools to control their populace, and non-state actors the ability to destabilize nations with a room full of cell phones. We live in a post-truth world where manufactured consent went from taking years to minutes.

Democracy requires informed consent.

Voting means nothing if the beliefs that drive votes are manufactured. A click farm can suppress a nation or galvanize it, microtarget a district, and turn neighbor against neighbor. It's the Twilight Zone episode where aliens flip lights on and off until everyone turns on each other with suspicion, except now you don't need a spaceship, just a social media page plugged into the algo.



Elections are swayed by algorithmic amplification. Public health undermined by recommendation engines boosting anti-vaccine content for engagement. Communities radicalized not by charismatic leaders but by feeds that learn what makes people angry and serve them more.

The mechanics are now documented. Researchers from NCRI traced the amplification pattern of some extreme political pundits in the U.S.: sixty-one percent of early retweets came from coordinated repeat accounts, nearly half the viral engagement originated from foreign bot farms in India, Pakistan, and Nigeria. Media coverage of one of the individuals receiving this amplification increased threefold as platforms interpreted synthetic engagement as organic legitimacy. Artificial visibility became real political influence – and most institutions still cannot detect the manipulation even when shown the evidence.[5]

Geopolitical diplomacy becomes impossible when populations believe incompatible realities; some leaders have even fallen for their own propaganda and begin making decisions based on it. Every aspiring authoritarian is watching closely. The playbook is being written in public. The tools are for sale on the open market - just add it to your cart, install, and control.

[5] Source: Same NCRI "America Last" report (Network Contagion Research Institute, December 2025, networkcontagion.us). Direct cite to this study — it contains all three statistics: 92% of earliest repeat retweeters from coordinated networks, ~50% of viral engagement from overseas clusters in India/Pakistan/Nigeria/Malaysia/Indonesia, and the 3x increase in media coverage as a result.

THE DARK POOL

Every data breach, every web scrape, every dataset sold between private and state data brokers feeds the same reservoir. Most people have no idea the scale of this unseen data market with all the databases from their nations for sale. This is the fuel for the algorithms.

Once data hits the pool, scale becomes irrelevant. The algo can zoom out to manipulate populations or zoom in to target a single person. A billion users or one user, same infrastructure, same tools.

The destination doesn't matter. Dark web dumps, broker markets, state acquisition. It all ends up in the same place: training sets, targeting databases, manipulation engines, surveillance systems, fraud, wealth extraction tools, geopolitical intelligence operations. Capitalism and statecraft drink from the same well. The distinction between advertising and influence operation is just who's paying. You are already in the pool.

Most people have no idea there's a shadow version of themselves distributed across databases in countries they've never visited, held by companies they've never heard of, feeding systems they'll never see to be used for targeting. Maybe you'll get an ad today, a drone strike tomorrow. [6]

[6] Source: General Michael Hayden (former NSA Director), public remarks at Johns Hopkins University, April 2014: "We kill people based on metadata." Plus The Intercept, Jeremy Scahill and Glenn Greenwald, "The NSA's Secret Role in the U.S. Assassination Program," February 10, 2014 — documenting how NSA metadata directly enables drone targeting.

ALGO-POLITICAL

The reactionary response is to build digital walls. GDPR. Social media application bans. Russia's RuNet. China's Great Firewall. Internet ID schemes. But walls don't contain algorithms, they just reshape the battlefield.[7]

Algorithmic control destabilizes the wielder too. These weapons are cheap and accessible. Similar to how drones have proliferated globally, now every state and non-state actor has access to the most effective physical and digital battlefield weapons ever created. Color revolutions that once took months now take hours, a few agents, a social media campaign, a march on the capital.

AI surveillance capitalism became the dominant mechanism for eroding sovereignty without firing a shot.

[7] Source: Margaret E. Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall* (Princeton University Press, 2018) — empirical study of how the Firewall reshapes rather than contains information flows. Plus ECFR, "Get Over Your X: A European Plan to Escape American Technology," Tobias Gehrke and José Ignacio Torreblanca, December 10, 2025 — on GDPR + EuroStack as reshaping rather than containing the algorithmic battlefield.

THE ASYMMETRIC CYCLE

Every dominant weapon system in history has generated its own countermeasure rendering it useless. Naval blockades ruled the seas until submarines made surface fleets sitting ducks; suddenly a handful of U-boats could sink entire armadas, rendering centuries of naval supremacy obsolete overnight.

The naval blockade was brought back in 2025 against a country that didn't have submarines, but they miscalculated that the cheap drone technology found its way to non-state actors and quickly sent the naval blockade (dumping millions of dollars of jet planes into the ocean on the way) back into the historical bin of ineffective geopolitical tools.

What would happen if we engaged the asymmetric cycle paradigm?

I challenge futurist and foresight thinkers to explore how to use this substrate, could it be used for peace? For enacting climate change futures now? Or tackling the other facets of the polycrisis we are currently in and new ones we will be facing soon.

SOURCES/ FURTHER READING

"Netanyahu Acknowledges Israel Losing Online Propaganda War" — *Times of Israel*, August 10, 2025

[Link](#)

"UN: Facebook Had a 'Role' in Rohingya Genocide" — *Al Jazeera*, March 2018

[Link](#)

"Palantir Sues Magazine That Revealed Switzerland Rejected Its Approaches" — *Financial Times*, February 2026

[Link](#)

"America Last: How Fuentes's Coordinated Raids and Foreign Fake-Speech Networks Inflate His Influence" — *Network Contagion Research Institute / Rutgers University*, December 2025

[Link](#)

"How Thomson Reuters Powers ICE and Palantir" — *Joseph Cox / 404 Media*, April 2026

[Link](#)

Author's Note: This article was drafted in late 2025, during a period when the Datafascism framework and Algorithm War thesis were still emerging. As of publication, many of the patterns described here have moved from prediction to documented reality. The next piece in the series will map these dynamics and address these new major events, and the emerging counter-infrastructure of democratic intelligence. Visualizing not only the architecture of the algorithmic battlefield but possible solutions and frameworks for organizations that want to navigate beyond it.

John Threat is a hacker, futurist, professor and global security advisor. He's lectured at the Kennedy Center on AI and University of Chicago, appeared on the cover of *Wired* and on *60 Minutes*, and been featured in *The Washington Post*. He founded *RIP SPACE*, an AI-native art/tech/culture studio in Los Angeles and recently produced the *Vibe Code Jam* in collaboration with *Rhizome* and *Anthropic*.

