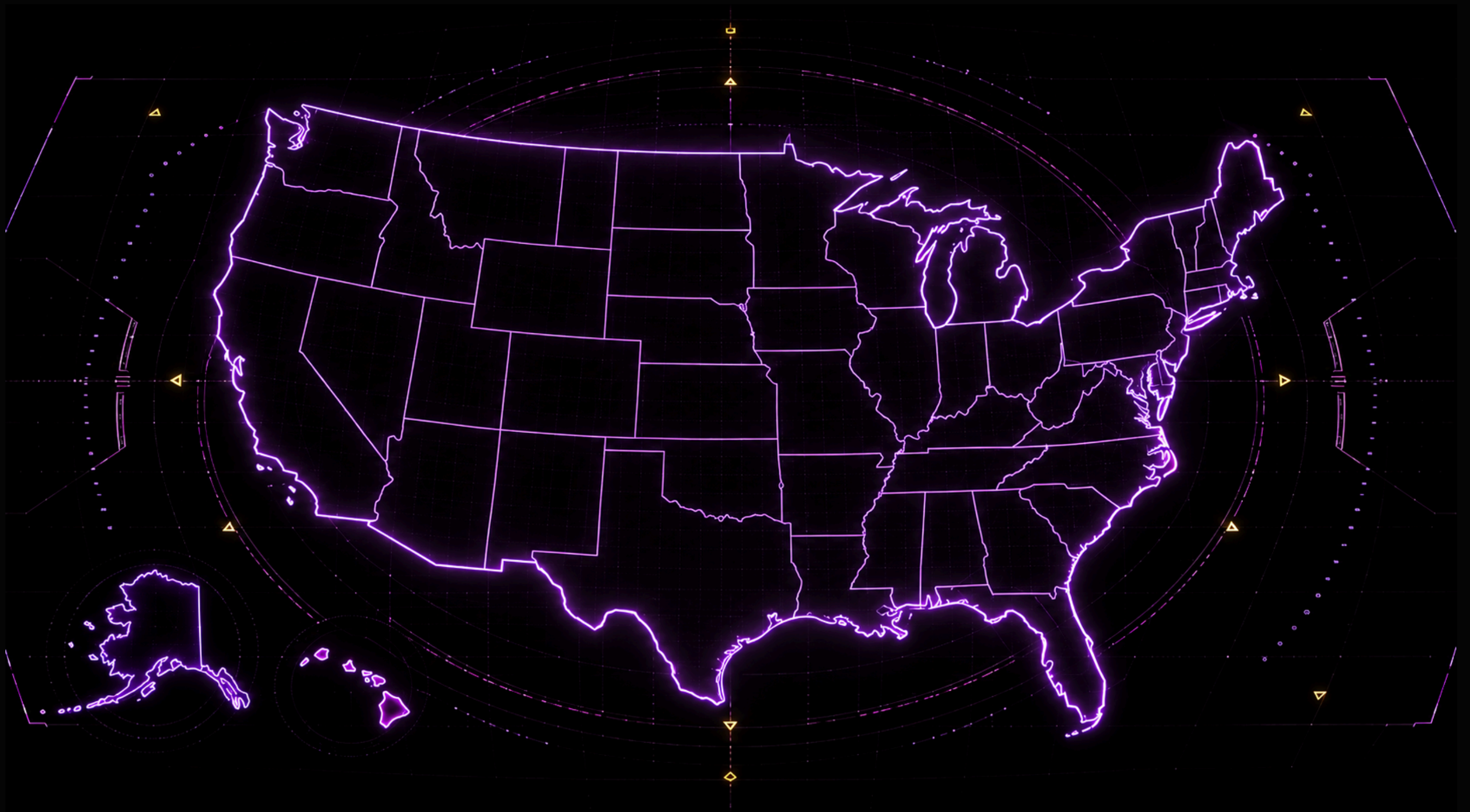




THE PROPAGANDA PLAYBOOK

**A Field Guide for Communities, Journalists,
and Creators to Survive the Storm**

PROPAGANDAPLAYBOOK.ORG

WHY THIS PLAYBOOK EXISTS

We are living in an era of propaganda, and the 2026 elections arrive at the most dangerous moment many communities have faced in the information environment in a generation. Three forces converged to produce this perpetual "propaganda storm."

Louisiana v. Callais [eviscerated](#) the Voting Rights Act that ended Jim Crow. Artificial intelligence, often rife with [bias](#), now [generates](#) convincing video, audio, and text at zero cost and infinite scale. Social media platforms operate with no guardrails, prioritizing [engagement](#) over [safety](#) and truth.

Black communities have stood at the center of this storm and their experience serves as the clearest map of how coordinated information warfare actually works. Reconstruction governments fell to [propaganda campaigns](#) that manufactured Black incapacity. The FBI's [COINTELPRO program](#) fabricated evidence to destroy Black leadership from the inside. When Black Lives Matter organizers demanded accountability, coordinated disinformation campaigns worked to reframe a civil rights movement as a public safety threat.

The 2026 election cycle will see information warfare deployed through tools no previous generation faced at this scale or speed.

Now, communities of every background operate inside the same information warfare infrastructure that Black communities learned to identify and resist long before it had a name.

This playbook exists because all of our communities, journalists, creators, and organizations deserve a field guide built for a perpetual propaganda storm. This storm runs continuously between elections and peaks during them. Every section covers a different phase: understanding the storm, what to build before the storm hits, how to move when it hits hardest, and how to construct infrastructure that outlasts any single season. Use it before, during, and after. Keep it close.

THREE FORCES OF PROPAGANDA STORM

Louisiana v. Callais

Eviscerated the
Voting Rights Act

AI at Scale

Zero-cost fabrication of
convincing media

Ungoverned Platforms

Engagement over
safety and truth

SIGNAL STATUS

Storm intensity:
ELEVATED

Information risk:
ACTIVE

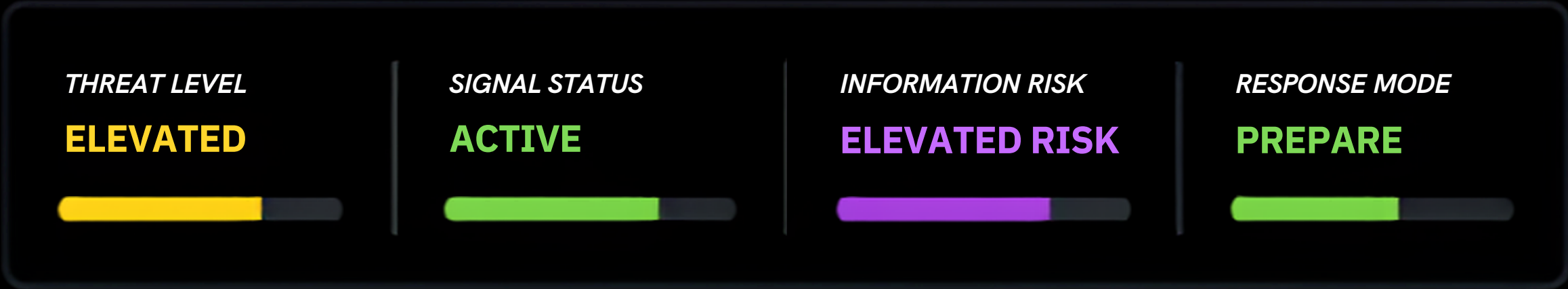
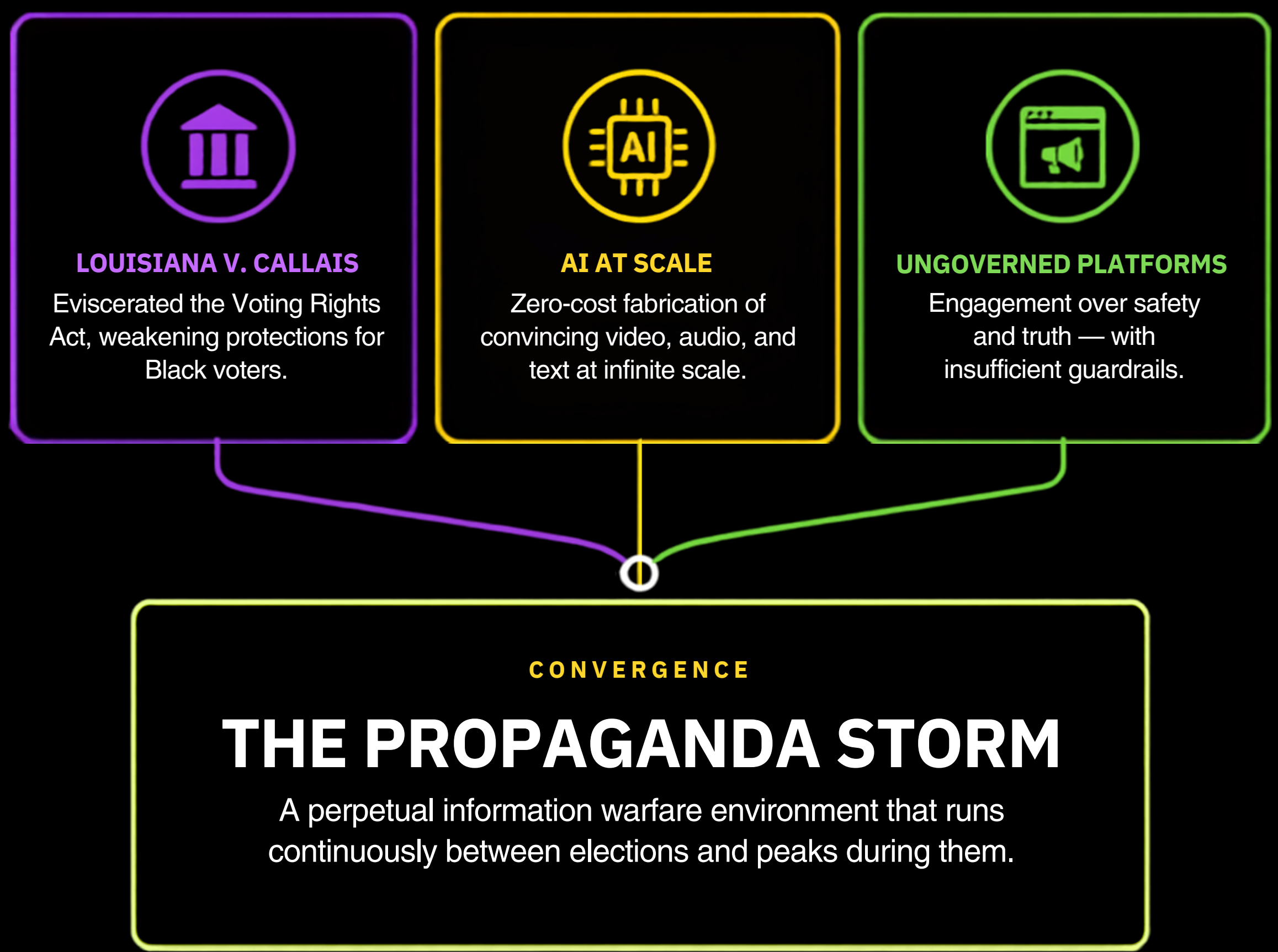
Response status:
PREPARE NOW

HOW TO USE THIS GUIDE

This playbook covers four phases: understanding the storm, building before it hits, responding when it does, and constructing lasting infrastructure.

ANATOMY OF THE PROPAGANDA STORM

Three forces converged to produce this perpetualpropaganda storm.





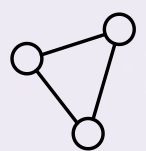
PART ONE

UNDERSTANDING THE PROPAGANDA STORM

*Every tactic below can intensify during periods of
elevated information risk. Knowing them now is
preparation.*

PROPAGANDA THREAT MATRIX

Four tactics. Each operates on a different target through a different mechanism toward the same outcome.

Tactic	Target	Mechanism	Outcome
 Manufactured Narratives	Reality itself	AI fabrication, context extraction, character destruction	Doubt & paralysis before communities can organize
 Infrastructure Destruction	Journalists, creators, institutions	Harassment, credibility attacks, platform suppression	Isolation — Arendt’s precondition for authoritarian control
 Wealth Extraction	Community trust networks	Fake directories, fabricated endorsements, fraudulent funds	Mutual aid dollars redirected away from legitimate organizations
 Cynicism Bombing	Black political participation	Weaponizes earned distrust, strips political context, amplifies confusion	Voter suppression similar to a fabricated attack

SHARED OUTCOME

A version of reality optimized to produce doubt and paralysis before communities can organize a response.

MANUFACTURED NARRATIVES

THEIR TACTIC

Information Manipulation

Coordinated actors manufacture the information environment our communities receive through three distinct techniques, AI fabrication, context extraction, and character destruction. All deliver the same outcome: a version of reality optimized to produce doubt and paralysis before communities and individuals can organize a response.

AI Fabrication

Artificial intelligence produces fabricated audio, video, and images that professional journalists struggle to authenticate under deadline pressure. The fabricated content spreads across platforms in hours. Corrections may take days to reach a fraction of the same audience.

IN A HIGH-RISK INFORMATION MOMENT:

*A manufactured video of a candidate admitting to voter fraud.
A fake audio clip of a civil rights director endorsing voter suppression legislation. A synthetically generated image of a polling location closing early in a majority-Black precinct. Each costs almost nothing to produce.*

Context Extraction

Context extraction deploys real content — genuine grief, documented injustice, verified outrage — as a weapon by removing everything that gives it meaning. The pain in the original content is real but the story constructed around it is fabricated.

Information Manipulation Includes:

- AI Fabrication
- Context Extraction
- Character Destruction

KEY INSIGHT

Corrections may take days to reach a fraction of the audience that receives fabricated content.

ANOTHER EXAMPLE

A video of police violence filmed three years ago in a different city circulates as breaking news the week before a local election. A Black creator's commentary on economic hardship gets clipped, stripped of its argument, and reposted by accounts whose entire purpose is manufacturing despair. These accounts require no fabrication budget. Platform algorithms reward the amplification of pain, so the technique costs nothing beyond the willingness to exploit it.

Character Destruction

Character destruction runs as a coordinated, multi-front campaign that strips a person of their credibility, livelihood, and humanity before the public ever scrutinizes what the state or a powerful actor did to them. It works because it operates across multiple arenas simultaneously, social, professional, legal, etc, creating the appearance of wrongdoing where none exists. When attacks arrive from enough different directions, or with the backing of the state, the conversation shifts from the crime to what the victim "should have done."

Repetition does the work that evidence cannot. A claim circulated across enough platforms or with the backing of the state acquires the texture of established fact. By the time any remedy or corrective action should occur, the target's humanity has already been systematically replaced by manufactured narratives.

INFRASTRUCTURE DESTRUCTION

THEIR TACTIC

INFORMATION ISOLATION

Hannah Arendt identified political isolation as the precondition for authoritarian control. Coordinated attacks on our communities target the infrastructure that prevents that isolation — the ability to generate accurate information, move it through trusted channels, and maintain the institutions that anchor collective knowledge. Journalists, creators, organizations, and institutions each carry a piece of that function.

REMEMBER

Repetition does the work that evidence cannot. A claim circulated across enough platforms or with the backing of the state acquires the texture of established fact.

WHEN A COORDINATED NARRATIVE BEGINS TO SPREAD:

A family demanding answers from the state watches coordinated negative reviews hit their business. The same week accounts begin to circulate claims about their character while the family is hit with defamation lawsuits or threats of lawsuits.

Journalists and Creator Credibility

Journalists do the verification work that keeps fabricated content from spreading unchallenged. Creators amplify verified information through the trust networks that our communities actually rely on. Coordinated [harassment](#) campaigns target the fear and [credibility](#) of both.

The mechanisms: Mass false reports flood their accounts in a smear campaign. Manufactured screenshots attribute statements they never made. Fabricated controversies reach their employers within hours. These campaigns peak when a journalist or creator tries to correct the record, slowing the people doing the work precisely when fabricated content spreads fastest.

Platform Suppression

Facebook's own internal [research](#) found that Black Instagram users faced account disabling at rates 50% higher than white users. Broader [research](#) across Facebook, Instagram, X, and YouTube puts that gap even higher, with Black users losing accounts at rates 60% above white users. During the George Floyd uprisings, Black creators [documented](#) platform throttling of protest coordination content while inflammatory counter-content climbed. Our communities built massive audiences on platforms that make unilateral decisions about what those audiences see. Platform algorithms suppress Black content during the moments it matters most, with no structural accountability to the communities affected.

Institutional Credibility

HBCUs, press outlets, and civil rights organizations connect individual Black community members to collective knowledge and collective power. Coordinated attacks manufacture [reasons](#) to distrust them. Disinformation campaigns [paint](#) HBCUs and Black civic organizations as elitist and incompatible with Black Christian values, driving wedges between Black institutions and the communities they serve. "Fake news" controversies get amplified and distorted through anonymous accounts. Coordinated review bombing targets Black-owned businesses during moments of community mobilization. When communities distrust their own institutions, the isolation deepens and feeds itself.

DATA NOTE

Platform-enforcement comparisons require a named population, period, baseline, source, and limitation. Remove any figure that cannot be verified in the approved research.

Do not treat a comparison with white users as a universal baseline unless the approved source supports that framing.

WEALTH EXTRACTION

THEIR TACTIC

CRISIS PROFITEERING

Every crisis that hits our communities, real or manufactured, generates an extraction opportunity for actors who position themselves inside community trust networks before the crisis arrives.

Community Level

These schemes arrive wrapped in cultural identity and community language because that framing lowers the verification instinct in people primed toward collective action and mutual support.

DURING PERIODS OF ELEVATED INFORMATION RISK:

A fake Black-owned business directory looks like genuine community infrastructure and collects payment information from members trying to support each other. A predatory cryptocurrency scheme carries fabricated endorsements from recognizable figures and circulates through financial empowerment spaces. A fraudulent relief fund uses real imagery from real disasters to redirect mutual aid dollars away from legitimate organizations. The schemes succeed because they imitate the real thing closely enough to pass in a moment of urgency.

Policy Level

Economic disinformation runs at the scale of policy. Distorted statistics about Black business failure rates, manufactured data about HBCU graduation outcomes, and false claims about the economic impact of majority-Black districts shape the funding and policy environment over years. Public and private investment gets redirected away from communities based on distorted and false evidence of institutional failure. The extraction lands at a scale no individual scheme reaches. See [The Blackout Report — Special Edition](#).

Extraction pathways

- Fake directories
- Fabricated endorsements
- Fraudulent relief funds
- Distorted policy statistics

CYNICISM BOMBING: THE MASTER TACTIC

THEIR TACTIC

Weaponizing Earned Distrust

Cynicism bombing converts legitimate Black political intelligence into a weapon against Black political participation.

The Senate Intelligence Committee [documented](#) coordinated Russian disinformation campaigns that peaked 60 days before both the 2016 and 2020 elections, targeting Black voters specifically with content engineered to confirm that electoral participation produces nothing. Those campaigns landed on ground that transactional politics had already [prepared](#).

Disinformation campaigns do not manufacture Black cynicism from nothing. Young Black adults who distrust the political process built that distrust from direct experience and accurate pattern recognition. Decades of transactional politics — campaigns that arrived in Black communities every two years with promises and left with votes and delivered little — produced genuine, earned skepticism.

Cynicism bombing locates that legitimate grievance, confirms it selectively, strips it of its political context, and amplifies it until it becomes the prevailing wisdom.

The 2026 cycle will likely run this tactic with *Louisiana v Callais* as its primary source material. The Supreme Court's [gutting](#) of the Voting Rights Act delivers factual confirmation that the system actively works against Black political participation. Cynicism bombing takes that fact, removes the organizing response it demands, and circulates only the conclusion. Counter-strategies that honor the intelligence underneath the cynicism and connect it to specific collective action with documented wins can help break the play.

Response timing

Cynicism campaigns exploit earned distrust and can intensify when communities are deciding whether and how to act.

COUNTER-STRATEGY

Honor the intelligence beneath the cynicism. Connect it to specific collective action with documented wins.

PLATFORM SUPPRESSION: THE DATA

Documented suppression of Black content across major platforms. These numbers should dominate the page.

FACEBOOK INTERNAL RESEARCH

50%

HIGHER

Black Instagram users faced account disabling at rates 50% higher than white users.

CROSS-PLATFORM RESEARCH

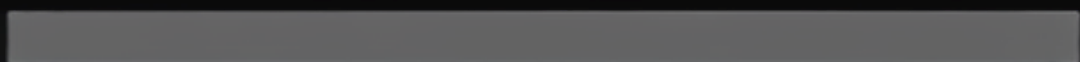
60%

ABOVE

Black users lose accounts at rates 60% above white users across Facebook, Instagram, X, and YouTube.

RELATIVE ACCOUNT DISABLING RATES

White users
(baseline)



1.0x

Black Instagram users (Facebook internal)



1.5x

Black users cross-platform



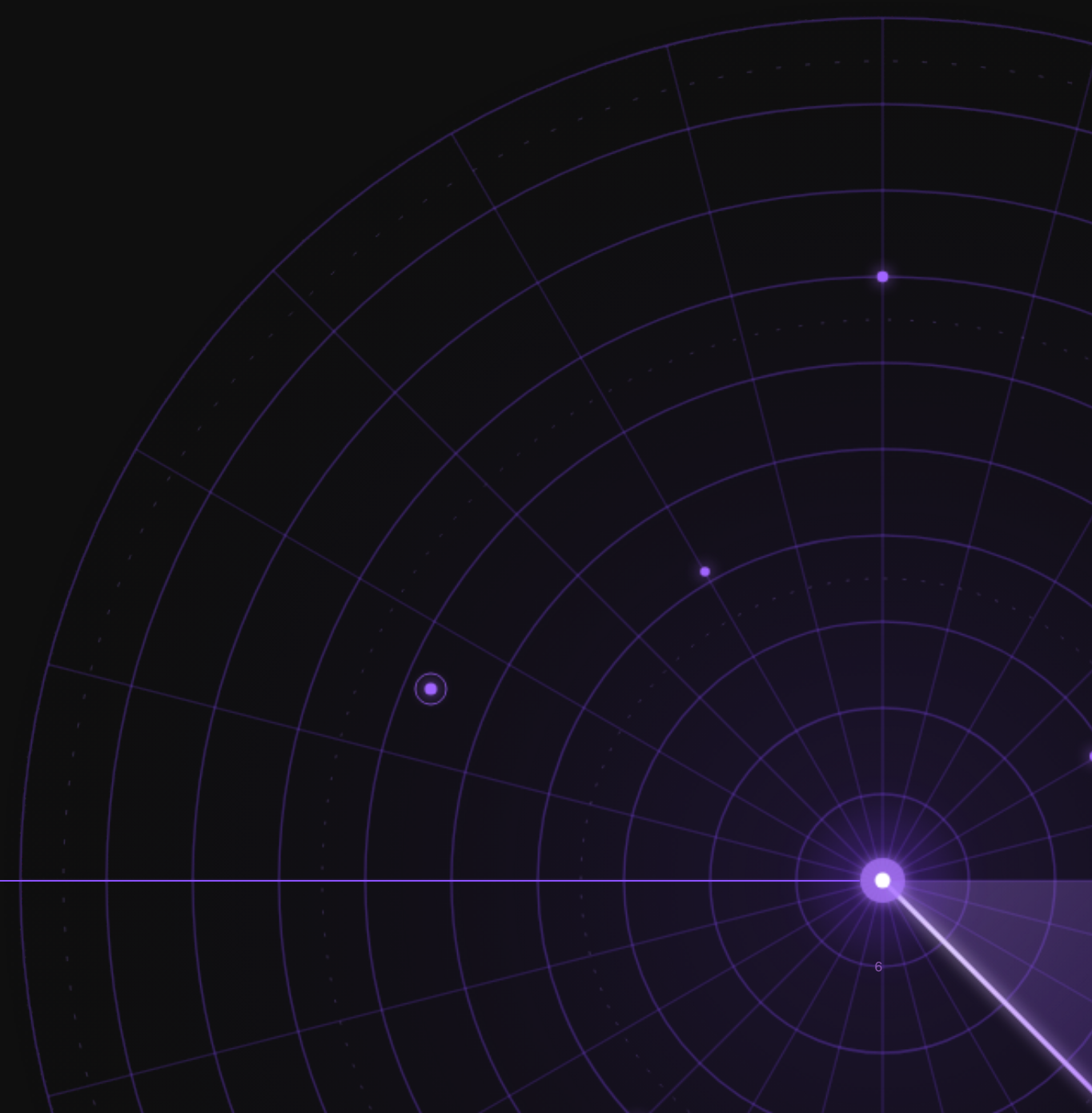
1.6x

During the George Floyd uprisings, Black creators documented platform throttling of protest coordination content while inflammatory counter-content climbed. Platform algorithms suppress Black content during the moments it matters most, with no structural accountability to the communities affected.

PART TWO

BEFORE THE STORM HITS

*Every preparation step below becomes more urgent
as a major event approaches. Build this infrastructure
before a crisis removes the time to build it.*



PREPARATION WINS

Amplification and repetition beat accuracy in a propaganda environment. A true story shared once loses to a fabricated story shared ten thousand times.

Pre-built, owned amplification networks that move verified information — including accurate voting logistics when relevant — help Black communities access trustworthy guidance. Build that infrastructure before a crisis arrives, using the timeline appropriate to your local context.

KNOW YOUR NUMBERS

Our Move:

Document Your Baseline Before Anyone Can Manufacture a New One

Coordinated attacks erase, suppress, and manufacture records.

In practice: Creators can lose account metrics when platforms suppress their content. Journalists can face fabricated professional histories. Organizations watch manufactured narratives circulate uncontested. A documented baseline makes every fabricated attack immediately verifiable as fabrication.

For Creators and Journalists

Screenshot and save your follower counts, engagement metrics, and platform analytics monthly. Store them somewhere you control — a personal drive, a secure cloud folder — not only on the platform itself. Build a personal website that tells your story and your background on your terms. When suppression hits, your documented baseline proves it.

For Organizations and Institutions

Tell your story loud, publicly, on your website and across platforms. Document your partnerships, your program results, and your community relationships before anyone manufactures a different version of them. Make the true narrative about who you are, what you do, and the communities you serve significantly easier to find than any future lie about you.

ACTION PRIORITY

Build documentation infrastructure **now**, before a crisis removes the time to build it.

DOCUMENT YOUR NUMBERS MONTHLY

- ✓ Follower counts
- ✓ Engagement metrics
- ✓ Platform analytics
- ✓ Partnership records
- ✓ Program outcomes

STACK YOUR AMPLIFIERS

Our Move: Build the Network That Moves Truth at Speed and Scale

Black communities already move culture faster than any platform algorithm can suppress when operating in coordination. Building strategic amplification infrastructure that is actively maintained converts that organic power into deliberate, protective infrastructure.

Digital Trust Map — online exercise

[The Digital Trust Map identifies](#) the people and channels that move information through a community. The web exercise is updated, completable online, and adaptable as platforms change. It helps you produce a practical network of reach, trust, validation, defense, and action.

- 1 Start with two questions.** Who are the audiences you need to reach during an election cycle and beyond? Who are the groups where a credibility attack does the most damage?
- 2 Do you currently reach those audiences at scale** and on the platforms they overindex to? Where are the gaps?
- 3 Identify credible actors inside each of those groups with significant reach.** Write down: (a) what platforms they hold audiences on, (b) what content they amplify most reliably, and (c) how quickly they can move when a crisis hits. Mapping this now, for offense and defense, means moving faster when it matters most.
- 4 Amplification alone may not hold during an attack.** Credibility support matters as well. Identify validators, peer organizations, and community leaders who can speak to your work publicly and quickly. A single spokesperson is a single point of failure. Build depth.

**DOES YOUR
REACH MATTER?
TAKE OUR TEST
TO FIND OUT!**



Your Signal Protocol

Decide in advance who receives the first signal when verified information needs to move, in what format, and through what channel. For example: Black press outlets get the first signal on breaking stories affecting Black communities. Verified content from Black journalists travels through the amplification network before unverified viral content does. These agreements require conversation and commitment now, before a moment of crisis removes the time to have them.

GET OFF RENTED LAND

Our Move: Own the Infrastructure Your Community Depends On

Documented [suppression](#) of Black content across major platforms confirms what Black creators and organizations have experienced directly — building exclusively on platforms someone else controls means platform decisions can erase years of community building overnight. Owned infrastructure survives those decisions.

Build Your Email List

An email or SMS list is a direct channel to people who have chosen to hear from you. Build durable access through newsletters, early information, community resources, direct member communications, websites, resource hubs, consented and secure community databases, trusted messengers, and locally controlled distribution partnerships.

Prioritize Community-Owned and Aligned Platforms

[Spill](#) was built specifically to create a safe, well-moderated space for Black communities online — with intentional algorithm and content moderation design to back that commitment. Download it. Build your presence there. A platform built for your community serves your community's interests when the larger platforms do not.

OWN YOUR LIST

Owned reach is measured by the people your organization can contact directly — not by a universal follower target.

% Press outlets

% Validators

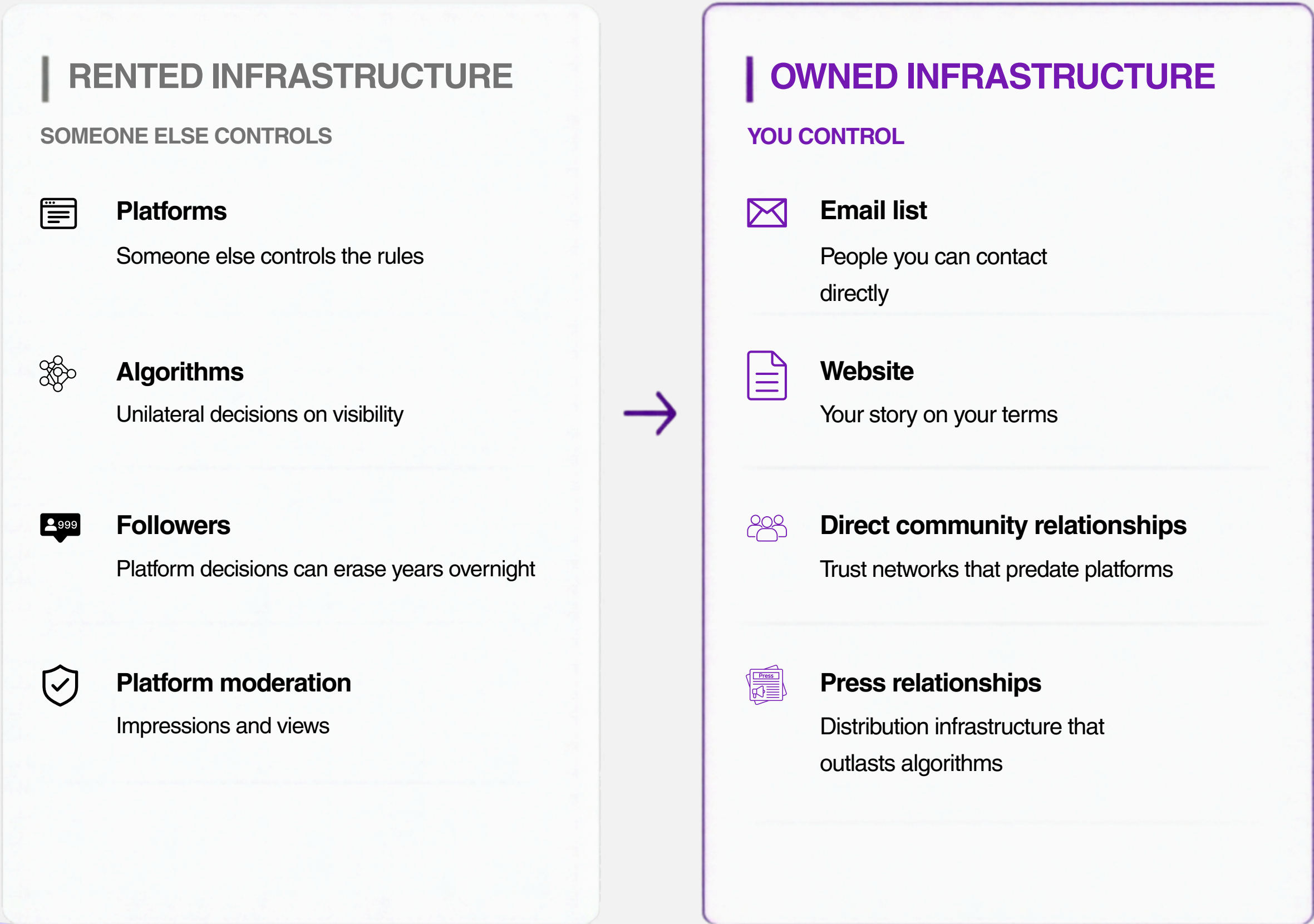
Peer organizations

Community leaders

% Email list

GET OFF RENTED LAND

Social media remains useful for discovery and distribution: "Get Off Rented Land" means building durable ways to reconnect with people directly when platforms change visibility, suspend accounts, or remove access.



Owned infrastructure survives platform decisions. Start building it now.

BUILD YOUR SAFETY NET

Our Move: Build What Holds You When the Storm Hits Hardest

Journalists, creators, and organizations under coordinated attack need verification tools, appeal processes, legal resources, and community relationships.

Verification Tools

These tools authenticate content and track how fabricated narratives spread:

- [InVID/WeVerify](#): browser extension for video authentication and metadata analysis
- [Google Reverse Image Search and TinEye](#): trace image origins and surface earlier appearances
- [Tech Transparency Project](#): tools to help track which tech companies are tracking you and which organizations are taking money from Big Tech
- [Bellingcat's Online Investigation Toolkit](#): open-source investigation resources used by professional journalists
- [Hoaxy](#): tracks how specific claims and fabricated stories spread across platforms

Appeals and Complaints

Document everything before you file anything. Screenshots, timestamps, and records of suppression, intimidation, threats of violence, or targeting matter even in a political environment hostile to platform accountability. They build the evidentiary record that future regulatory action and legal challenges depend on.

- [Electronic Frontier Foundation](#): legal referral network for digital rights violations
- [Freedom of the Press Foundation](#): digital security resources and legal support specifically for journalists

DOCUMENT FIRST

Screenshots, timestamps, and records of suppression build the evidentiary record that future accountability depends on.

- [FTC complaint portal](#): for fraudulent schemes, fake directories, and predatory financial targeting
- [Election Protection](#): provides a voter assistance hotline for reports of voter suppression, intimidation, or misinformation affecting voting access. Can connect individuals with legal resources and election attorneys.

Cultivate Trusted Press Relationships

Black press outlets provide distribution infrastructure that predates every social media platform and will outlast every algorithm change. An established relationship with Black press holds a publication channel that platform suppression cannot close. Build those relationships before you need them.

- **Download [Aisha](#)** at aisha.ai, type in your state, and get a curated list of Black news organizations to follow, subscribe to, and reach out to directly. Aisha is a digital AI assistant built by [Onyx Impact](#) that prioritizes vetted sources, privacy, and environmental awareness.
- **Subscribe and pay for Black media directly:** revenue keeps independent journalism alive

Build Your Resilience Network

Black journalists, creators, and community leaders who have already navigated coordinated disinformation attacks carry knowledge that no document fully captures. The organizations below hold networks of people who have been through it and stayed through the recovery. Connect with them now.

- [National Association of Black Journalists \(NABJ\)](#): digital defense resources, peer networks, and rapid response support for Black journalists under attack
- [Lawyers Committee for Civil Rights Under Law](#): operates legal and policy initiatives focused on protecting civil rights online and offline

RESILIENCE ORGS

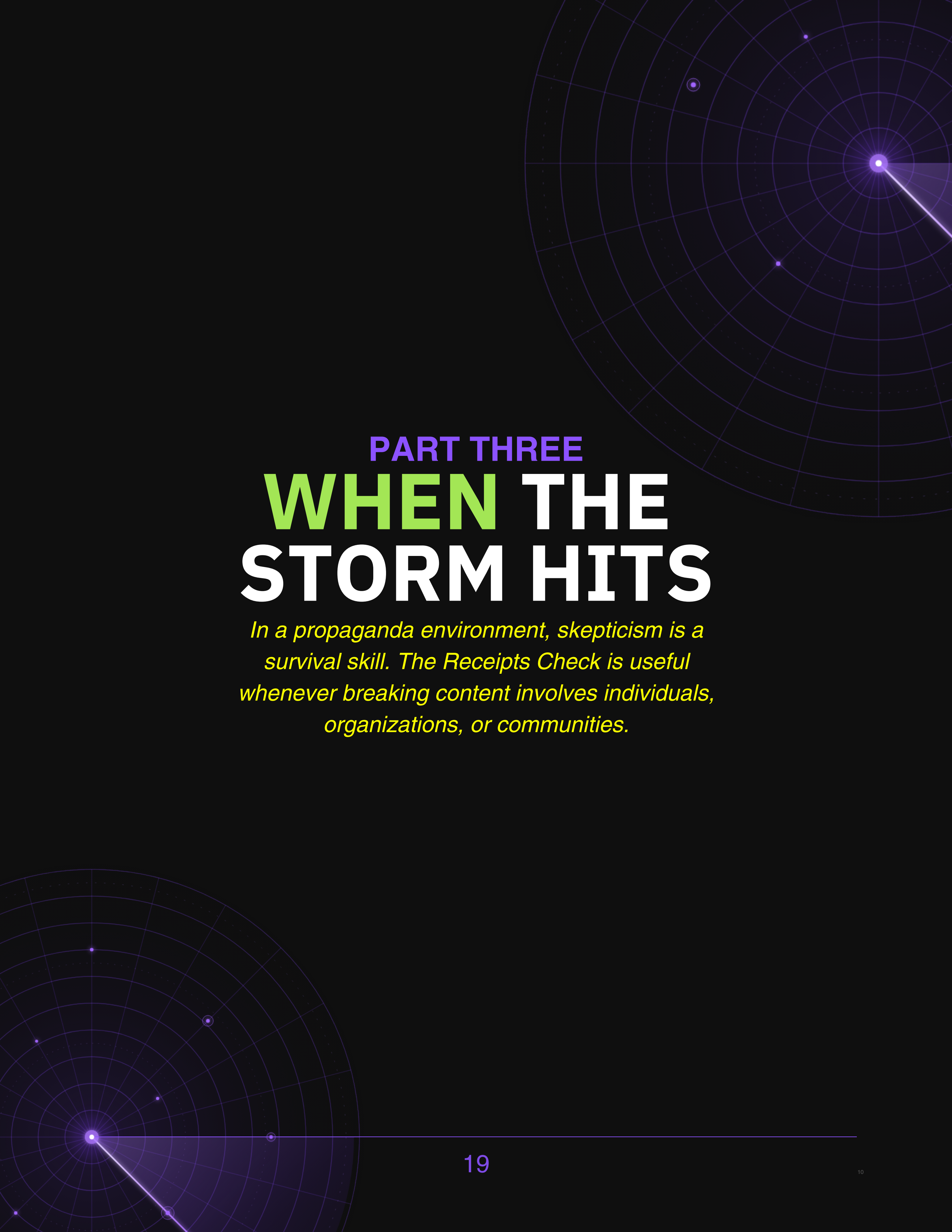
- [NABJ](#)
- [PEN America](#)
- [Color Of Change](#)
- [Lawyers Committee](#)
- [Algorithmic Justice League](#)
- [Coalition Against Online Violence](#)

- [Color Of Change](#): campaigns and advocacy infrastructure for Black communities facing coordinated targeting
- [Algorithmic Justice League](#): research, advocacy, and community resources on algorithmic suppression and bias
- [PEN America's Online Harassment Field Manual](#): comprehensive resource for creators and journalists facing coordinated harassment
- [Coalition Against Online Violence](#): direct support for journalists and creators targeted by online abuse campaigns

✦ IF YOU ARE AT RISK ✦

The resources above address information threats. The resources below address what happens when a coordinated attack escalates into physical, legal, and digital danger simultaneously. Build these relationships before you need them.

- Before an attack: [Democracy Security Project](#): proactive risk assessment, cyber safety, physical security planning, and direct support for individuals and organizations operating in high-threat environments.
- Under active attack: [Democracy Protection Network](#): physical security, cybersecurity, crisis communications, and legal representation for individuals and organizations already under coordinated threat. DPN links directly to [Protect Democracy's Nonprofit Toolkit](#) for organizations facing politicized government investigations.
- When it escalates beyond your capacity: [Beacon](#): free, high-touch crisis response for individuals and organizations facing simultaneous legal, reputational, digital, and physical threats. Intake at beacon.us. Response may take up to three days; Beacon does not provide emergency services.



PART THREE

WHEN THE STORM HITS

In a propaganda environment, skepticism is a survival skill. The Receipts Check is useful whenever breaking content involves individuals, organizations, or communities.

Our Move: Be Skeptical

In a propaganda environment, skepticism is a survival skill. The Receipt Check is a three-question protocol that runs on any breaking content involving individuals, organizations, or communities before your network amplifies it. In a crisis moment, when emotion runs high and content moves fast, these three questions limit risk and ensure you remain a credible source for your community.

THE RECEIPTS CHECK

1. Can you verify the source independently?

Trace the content to its origin. Find the actual post on the actual account. Pull the primary source directly and confirm the content exists in its original context and says what the circulating post claims it says. In a crisis or propaganda moment, the source is often the only thing that can be independently confirmed when everything else moves too fast to verify.

2. What does this content ask you to feel before it gives you facts?

Manufactured content sequences emotion before evidence: outrage, despair, shame, urgency, etc demanding immediate action. Legitimate coverage delivers verified facts first and emotional weight follows from them. Content that reverses that sequence warrants a pause before it travels through your network.

3. Who benefits from this story circulating right now?

Timing and pattern can reveal an operational goal. Ask whose strategic interest the story serves before your network moves it.

THREE QUESTIONS

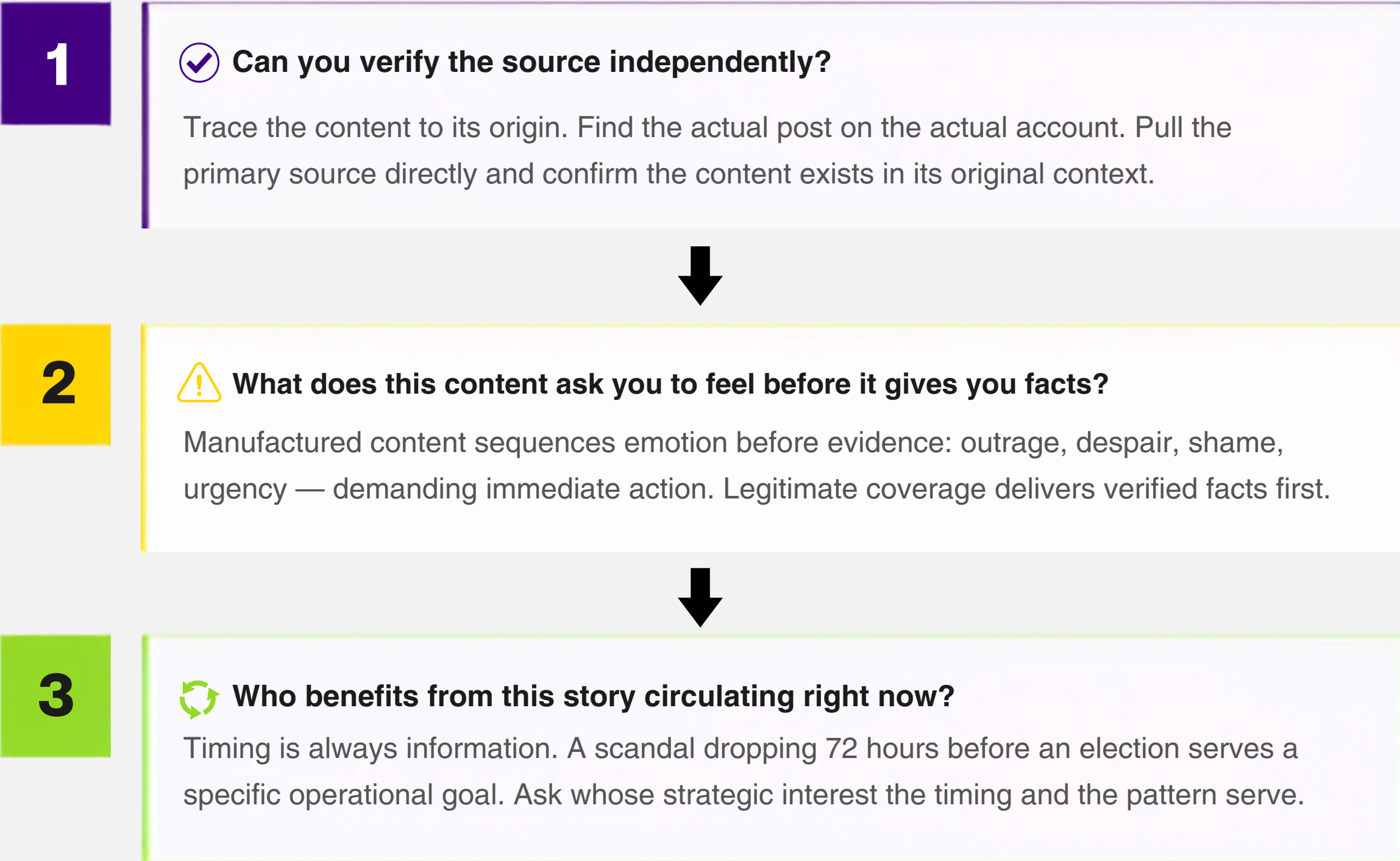
- ☐ Can I verify the source?
- ☐ Does it hit feelings before facts?
- ☐ Who benefits right now?

CRITICAL INSIGHT

Content that sequences emotion before evidence warrants a pause before it travels through your network.

THE RECEIPTS CHECK

A three-question protocol that runs on any breaking content before your network amplifies it. In a crisis moment, these three questions limit risk and ensure you remain a credible source.





VERIFY BEFORE AMPLIFYING

IF EVEN ONE ANSWER GIVES YOU PAUSE

Hold off on sharing with your wider network.

WHEN REACH IS UNCLEAR

Verify before you amplify. A contained threat broadcast may quickly become wide reach.

ACTIVATION PROTOCOL

Our Move: Always Step With Intention

When a propaganda attack drops, your Part Two infrastructure activates in sequence. If you are reading this in the middle of a crisis, start at Step 1 and move through each step in order.

1

RUN THE RECEIPT CHECK

Before anything moves through your network, the Receipt Check should run. Pull the primary source directly. Run [InVID/WeVerify](#) on any video. [Run Google Reverse Image Search and TinEye](#) on any images. Amplifiers in your network should hold until the content clears.

2

DEPLOY YOUR VALIDATORS AND MOVE THE VERIFIED STORY

Your validators and peer organizations from your digital trust map respond publicly. Contact them directly and specifically: name what you need, name the timeline. Simultaneously, call trusted outlets to provide the verified story if applicable. Then distribute through your email list immediately after. If platforms suppress your content during an active attack, your press relationships and owned infrastructure carry the verified story directly to your community.

3

ACTIVATE YOUR RESILIENCE NETWORK

If the attack targets you directly, activate your resilience network now. [NABJ rapid response](#). [PEN America's Online Harassment Field Manual](#). [Coalition Against Online Violence direct support](#). These relationships exist in your safety net because building them mid-attack costs time you may not have. If the attack combines legal, physical, and digital threats simultaneously, contact [DPN](#) and/or [Beacon](#) through your safety net resources in Part 2.

4

DOCUMENT EVERYTHING

Screenshots. Timestamps. Records of suppression, harassment, and fabrication patterns. Documentation builds the evidentiary record that platform appeals, legal challenges, and future accountability actions depend on. File platform complaints through the [EFF](#) and [Freedom of the Press Foundation](#) channels. Share what you document with your resilience network so the pattern becomes collective evidence.

THE ACTIVATION PROTOCOL

When a propaganda attack drops, your Part Two infrastructure activates in sequence. Start at Step 1 and move through each step in order.



RUN THE RECEIPT CHECK

Pull the primary source. Run InVID/WeVerify on video. Run reverse image search. Amplifiers hold until content clears.



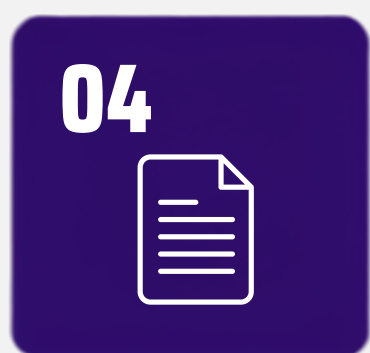
DEPLOY YOUR VALIDATORS

Validators and peer organizations respond publicly. Call trusted outlets. Distribute through your email list immediately after.



ACTIVATE YOUR RESILIENCE NETWORK

NABJ rapid response. PEN America. Coalition Against Online Violence. If combined threats, contact DPN / Beacon.



DOCUMENT EVERYTHING

Screenshots. Timestamps. Records of suppression. File complaints through EFF and Freedom of the Press Foundation.

THE ELECTION PROTOCOL

Our Move: Know Response Priorities

Every tactic from Part One can require a different response level. Given that resources are finite, the Response Framework below tells you where to direct energy first.

RESPONSE LEVELS

- CONTAINED
- MID-LEVEL
- WIDE REACH

The Reach Calibration Rule

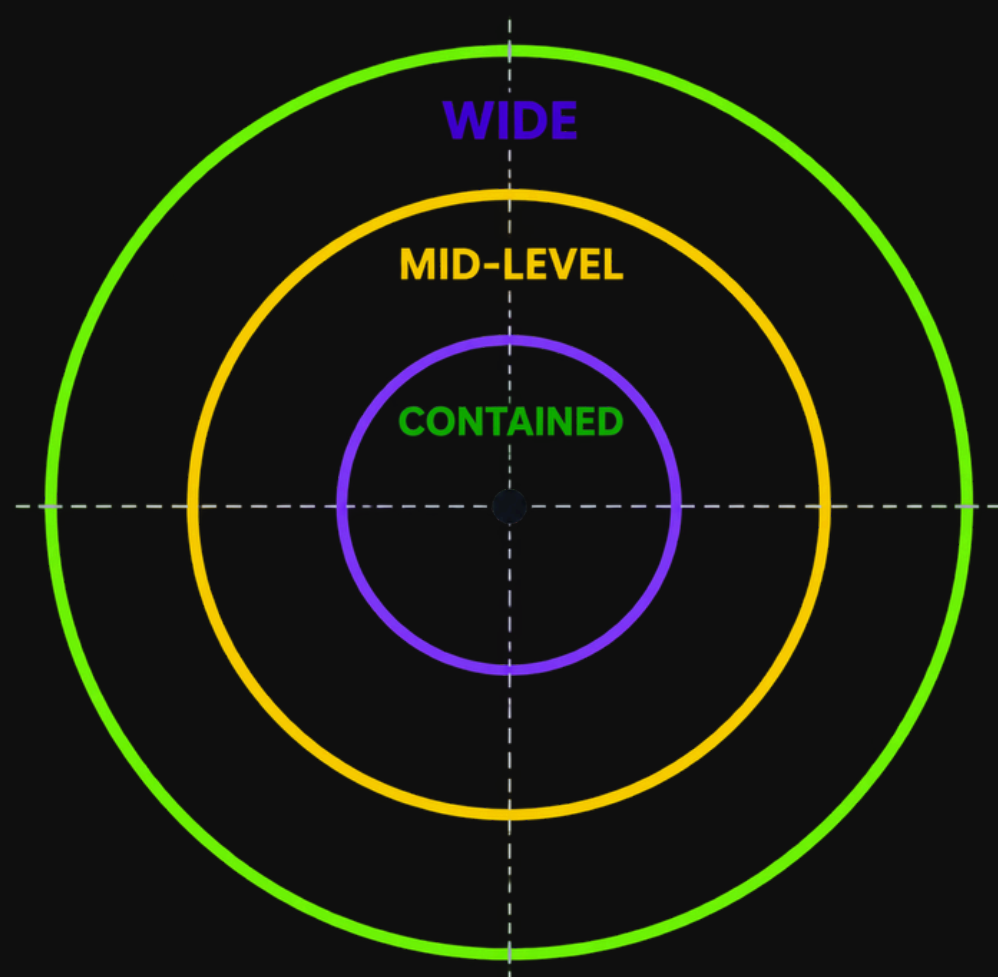
Full mobilization carries real risk. Amplifying unverified content through a large network spreads the original misinformation faster than the correction travels. Community attention is also finite. **Over-activation trains your network to tune out**, and when you need full mobilization, your signal lands soft. **Calibrate your response to the actual reach of the threat before you move.**

- **Contained reach** — describes misinformation circulating in a small group, or a limited local network. It calls for a direct, quiet correction through your most trusted local validators. Verified information goes to the people closest to the source, while the broader amplification network stays quiet.
- **Mid-level reach** — describes misinformation spreading across multiple platforms or communities, picking up shares and velocity. It calls for your signal protocol and your press relationships. Verified information moves through those channels with your validators attached. The Activation Protocol stays on standby.
- **Wide reach** — describes misinformation running across major platforms, generating significant engagement, or targeting a specific high-stakes moment like a polling location or mail ballot deadline. It calls for the full Activation Protocol. Verified information travels through your entire amplification network and email list immediately.

When reach levels are unclear, **verify before you amplify**. A contained threat that you broadcast may quickly become a mid-level or wide reach thread.

THE REACH CALIBRATION RULE

Calibrate your response to the actual reach of the threat before you move. Over-activation trains your network to tune out.



■ CONTAINED REACH

Misinformation circulating in a small group or limited local network

→ **Direct, quiet correction through your most trusted local validators**

■ MID-LEVEL REACH

Spreading across multiple platforms or communities, picking up shares and velocity

→ **Signal protocol and press relationships. Validators attached. Activation Protocol on standby.**

■ WIDE REACH

Running across major platforms, significant engagement, or targeting a high-stakes moment

→ **Full Activation Protocol. Verified information through your entire network and email list.**

Verify before you amplify.

A contained threat that you broadcast may quickly become a mid-level or wide reach threat.

VERY HIGH PRIORITY

FALSE VOTING LOGISTICS

Misinformation about polling locations, hours, ID requirements, mail ballot deadlines, and drop box locations directly prevents Black voters from casting ballots. A voter who shows up at the wrong location or the wrong time loses their vote entirely. **No other category of election misinformation produces that immediate, irreversible outcome.**

Note: voting logistics vary by jurisdiction. Verify polling locations, hours, identification requirements, mail-ballot rules, return deadlines, and drop-box locations with the appropriate official source for the local context. Do not treat early voting, in-person absentee voting, mail voting, and Election Day voting as interchangeable.

Verified sources for voting logistics. Use all three, because they serve different needs:

[Vote.org](#) — delivers plain language registration deadlines, ID requirements, polling locations, and mail ballot information across all 50 states. Start here for fast, clear answers your community can act on immediately.

[Your state's official Board of Elections website](#) — carries the primary legal authority for your jurisdiction. Requirements and deadlines here are binding. Some state election websites, particularly across the South, present this information in ways that require navigation experience to use effectively. Cross-reference with Vote.org when the BOE site produces confusion.

[Election Protection hotline: 1-866-OUR-VOTE](#) — connects voters experiencing problems, misinformation, or interference at any point in the voting process to live legal support. Distribute this number widely through your owned infrastructure before Election Day and keep it circulating through the full voting window.

IRREVERSIBLE OUTCOME

A voter at the wrong location or wrong time loses their vote entirely.

HOTLINE

1-866-OUR-VOTE

14

HIGH PRIORITY

INTIMIDATION THEATER AT POLLING LOCATIONS

Law enforcement presence at or near polling locations, ICE activity in surrounding areas, and armed civilian groups positioned near polling sites generate fear that translates directly into suppression. The tactic runs digitally as well. In 2024, mass [racist](#) text messages circulated through Black communities warning of the KKK arriving at polling locations. The physical presence and the digital threat operate together, producing fear before voters leave the house.

Poll workers and election officials hold authority inside polling places. **The Election Protection hotline at 1-866-OUR-VOTE** connects voters experiencing intimidation to immediate legal support. When digital intimidation content reaches wide circulation, counter-messaging travels through your full network alongside the hotline number, moving fast enough to land before voters make decisions about whether to show up.

The content arrives formatted to trigger protective instincts: warnings about armed groups, threats at specific polling locations, urgent alerts about ICE activity in neighborhoods. **TREAD CAREFULLY:** It looks like information your community needs immediately. It arrives from accounts that appear credible or from people in your own network who already amplified it without verifying. The fear it generates is real even when the threat is fabricated. **A creator who shares it to protect their community becomes the distribution network the theater requires.**

Make sure to run the Receipt Check on any election-related threat content before it touches your platform. When a peer creator amplifies false intimidation content, your direct message carrying verified information travels to them immediately, and your own counter-messaging runs on your platform at the same time. Retraction requests move slowly and often fail entirely during high-volume election periods. Your counter-messaging reaches your community regardless of how the peer responds.

CREATOR ALERT:

Creators with large platforms are a primary target of intimidation theater.

The primary targets of intimidation theater moving forward. Creators with large platforms are a primary target of intimidation theater. TREAD CAREFULLY. Fake warnings about armed groups, polling location threats, and ICE activity arrive built to trigger your protective instincts, often from accounts or peers who already believe them. Run the Receipt Check before any election-related threat is amplified on your platform. Read the playbook to learn more.

READ CAREFULLY

A creator who shares intimidation theater to protect their community becomes the distribution network the theater requires.

HIGH PRIORITY

FABRICATED ATTACKS ON BLACK LEADERS AND ORGANIZATIONS

Coordinated fabrications targeting Black civic organizations and community leaders accelerate in the final 30 days before an election, timed to land when correction capacity sits lowest. Apply the Reach Calibration Rule the moment an attack appears. Your documented baseline from Part Two, including leadership and program outcomes alongside public statements, activates once reach level confirms full mobilization. The Activation Protocol runs in full. The documented record travels your signal protocol and lands with credibility only when you have spent the time building your narrative loudly and clearly across platforms ahead of the attack window.

HIGH PRIORITY

CYNICISM BOMBING DURING THE ELECTION CYCLE

Cynicism bombing weaponizes real political grievance to deliver a single conclusion: that Black political participation produces nothing. During the days and weeks before and election, it functions as voter suppression and is calibrated to produce the same outcome. Its damage extends well past Election Day, which places it on the high priority list now and keeps it there beyond the cycle.

The Receipt Check can help catch this at source verification. Content tracing to anonymous accounts with no prior community history, arriving with manufactured urgency at peak mobilization moments, signals the tactic is running. At wide reach, counter-messaging travels through your amplification network immediately, leading with specific, documented wins from Black collective action through your owned infrastructure and Black press relationships.

ATTACK WINDOW

Coordinated attacks can intensify when correction capacity is low.

FALSE VOTING LOGISTICS

IRREVERSIBLE OUTCOME

A voter who shows up at the wrong location or the wrong time loses their vote entirely. No other category of election misinformation produces that immediate, irreversible outcome.



Polling
locations



Hours



ID
requirements



Mail ballot
deadlines



Drop box
locations

MAIL VOTING TIMELINE

RISK

Always verify requirements and deadlines
for voting with official sources.



ELECTION PROTECTION HOTLINE

Live support for voters experiencing
problems, misinformation, or interference.

1-866-OUR-VOTE

TRUSTED RESOURCES



Vote.org

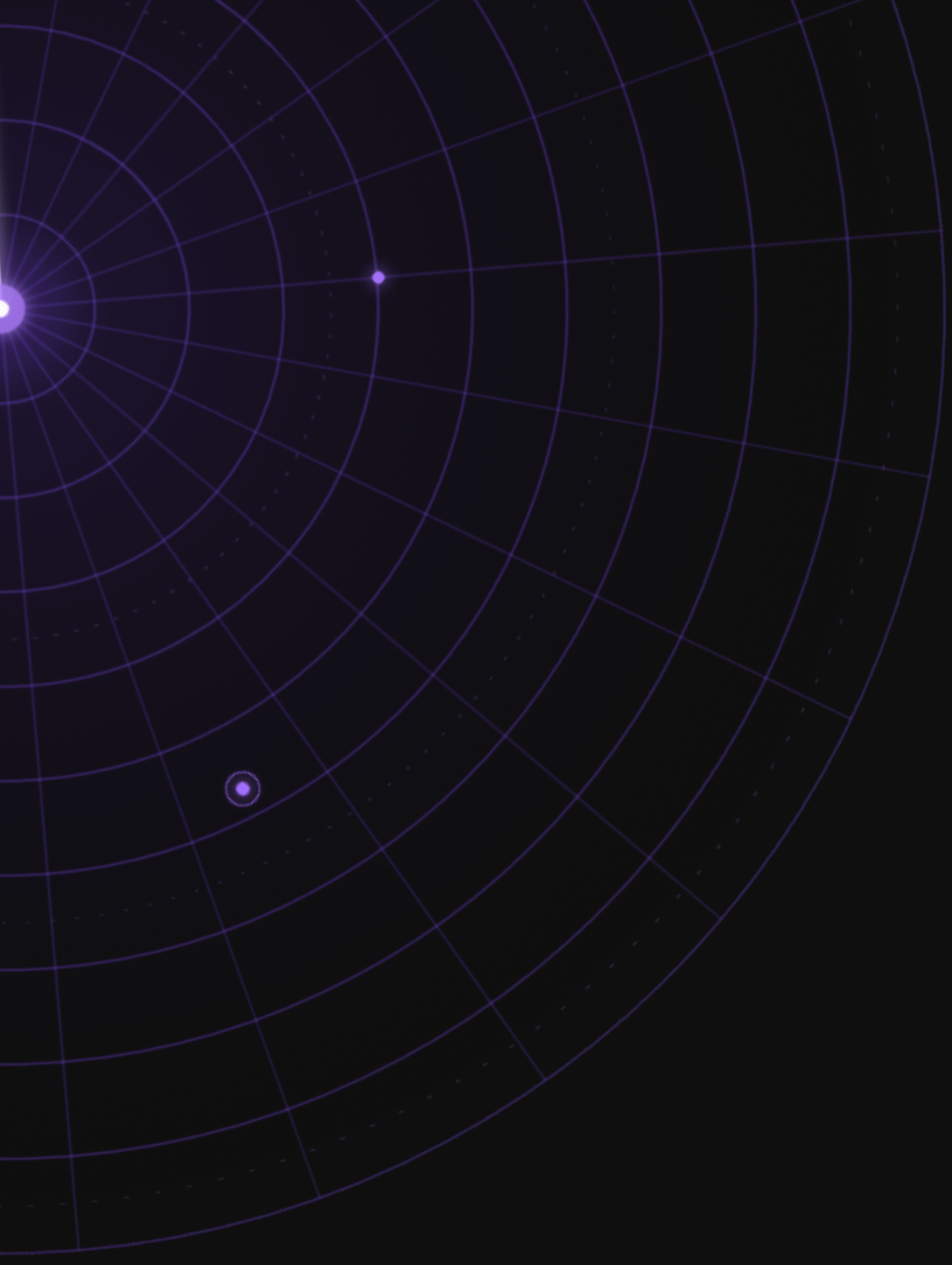
Plain language deadlines,
ID, locations

State BOE

Primary legal authority —
binding

1-866-OUR-VOTE

Live legal support



PART FOUR BUILD WHAT LASTS

The documentation, networks, and hard knowledge earned under fire become the foundation for fights that outlast any single attack. Part Four is where survival converts into structural power.

STRUCTURAL ACTION

Push candidates, state officials, election administrators, and organizations toward four concrete commitments.

IMMEDIATE PRIORITIES

01 CLASSIFY AS VOTER SUPPRESSION

Classify coordinated digital disinformation targeting Black voters as voter suppression under state law. Direct state attorneys general to investigate and prosecute.

02 SAFEGUARDS ON AI IN ELECTIONS

Prohibitions on deceptive synthetic media or disclosure requirements for AI-generated content in elections.

03 FUND LOCAL BLACK PRESS

Encourage funding of local Black press outlets and trusted community information networks as essential election infrastructure.

04 RAPID RESPONSE PROTOCOLS

Establish rapid response protocols between state election officials and community organizations so disinformation triggers immediate, thoughtful response.

LONG-TERM PRIORITIES

FEDERAL CIVIL RIGHTS LEGISLATION

Treat racially targeted algorithmic suppression as a civil rights violation with private right of action — meaning affected communities can sue, not just petition.

COMMUNITY-CONTROLLED INFRASTRUCTURE

Community-owned platforms, Black press sustainability funds, and shared verification networks that do not depend on the goodwill of the same platforms running the disinformation.

The organized expression of a people that read the playbook, recognized the plays, and built something to endure and overcome the storm.

IMPACT-BASED RECOVERY

A sustained propaganda storm exhausts the people fighting it by design. Recovery rebuilds capacity deliberately and in sequence.

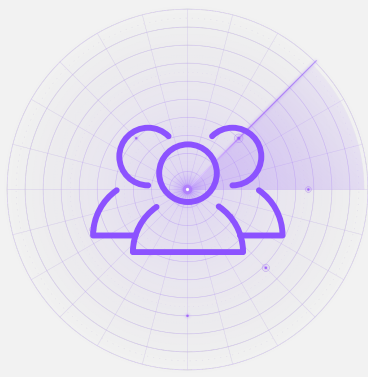
Start With Network Capacity

The community organizations, amplification networks, legal contacts, and trusted partners that activated during the crisis need sustained investment after it, including: real dollars, regular communication, shared resources, collaborative projects that keep the network warm and ready.

Again, make sure you have documented what happened thoroughly. Which platforms amplified the attack fastest? What types of harm were experienced? Which verification tools slowed the spread? Which community responses moved the needle? That documentation belongs in a shared resource accessible to the next organizer, family, journalist facing the same playbook. This is how we build and circulate institutional knowledge.

Material Support for Survivors

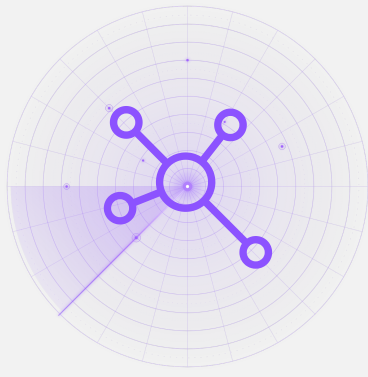
Character destruction campaigns cause real economic harm and reputational damage that persists long after the campaign ends. Recovery means organizing material support for survivors: fundraising, legal defense networks, business referral campaigns through community networks, and sustained public affirmation from credible voices long after the news cycle moves on.



SUPPORT SURVIVORS

Keep partners connected.
Fund the infrastructure.
Document what worked.

- LEGAL
- FUNDRAISING
- REFERRALS
- PUBLIC SUPPORT



REBUILD THE NETWORK

Organize legal support, fundraising, referrals, and long-tail public affirmation.

- PEOPLE
- FUNDING
- DOCUMENTATION
- SHARED RESOURCES

THE STRUCTURAL FIGHT: R.I.S.E.

Propaganda storms, fueled by AI and related technologies threaten racially inclusive democracy at the infrastructure level. Our communities bear the concentrated harm of systems designed without them in mind. These are the specific demands worth carrying into every room with the power to act on them. R.I.S.E.

Regulatory and Legislative Action

We can not build safer information ecosystems by relying on communities to clean up the damage after it happens. Lasting change requires regulatory and legislative action both at the state and federal level that shifts accountability upstream. Reforms should put meaningful safeguards on design choices, business practices, and systems that enable harmful content to spread unchecked.

Key legislative priorities include:

- **Researcher access to data:** Independent researchers should have meaningful access to platform and AI system data needed to identify emerging harms, assess disparate impact, and evaluate how harmful content spreads. The [Platform Accountability and Transparency Act](#) at the federal level, is a model framework which compels platforms to share data with researchers studying coordinated disinformation.
- **Algorithmic accountability:** Require greater transparency, testing, and accountability for recommendation and algorithmic systems that amplify the reach of harmful content. The [Algorithmic Accountability Act](#) is a model framework that requires platforms to conduct impact assessments of automated decision systems.
- **AI disclosure:** Legislation should establish clear disclosure and labeling requirements for deepfakes and other manipulated media in high-risk contexts such as where synthetic content could undermine elections. For example, over [30 states](#) have passed laws regulating or restricting the use of AI deepfakes in elections.

Investigations and Enforcement

Strong laws mean little without mechanisms to enforce them. Stakeholders should identify institutions that can investigate technology-enabled harms and strengthen accountability. This is also where the documentation of harms and preservation of evidence becomes critical. Consistent records of what happened, how harmful content was spread, and the resulting harm can support investigations and potential litigation.

Potential pathways include:

- **State Enforcement:** Engage state attorneys general with relevant consumer protection, civil rights, and technology authorities.
- **Private Litigation:** Consider whether existing laws or emerging legal theories provide for individuals or organizations to pursue private litigation.
- **Research and Watchdog Efforts:** Partner with independent researchers and watchdog organizations that can establish evidence of systemic failures and support litigation.

Strategic Corporate Accountability

Corporate accountability is strongest when stakeholders can turn documented harms into targeted pressure that can influence a company's behavior. Rather than relying solely on public criticism or asking platforms to voluntarily change, identify the company's pressure points and build campaigns around specific, achievable demands.

Stakeholders can:

Mobilize advertisers: Engage major advertisers and corporate partners that may not want their brands associated with platforms that facilitate racialized harms.

Build collective economic pressure: Advertisers moved faster than regulators during every major platform accountability moment of the last decade. A standing coalition of Black economic organizations, civil rights groups, and creator networks, again, ready to activate within 72 hours of a documented coordinated attack, converts economic pressure from a reactive tool into a permanent structural lever.

ECONOMIC LEVER

Advertisers moved faster than regulators during every major platform accountability moment of the last decade.

72-HOUR STANDARD

A coalition ready to activate within 72 hours of a documented attack converts economic pressure into a permanent structural lever.

Target specific corporate decisions: Focus campaigns on concrete changes such as modifying recommendation algorithms, strengthening AI safeguards, or increasing transparency, particularly where there is a legislative vehicle.

Demand dedicated escalation channels: Journalists, creators, and community organizations need designated escalation channels with specific contacts, specific response timelines, and specific accountability, not general content moderation queues that bury urgent cases in algorithmic backlog.

Empowering Communities

The first three parts of R.I.S.E. bend towards getting structural changes to the design decisions made inside these companies. What gets recommended, who gets targeted and what an AI model is allowed to generate are decisions made by a small number of people with Black voices rarely in the room.

Legislation and enforcement can force a company to change a design choice. Sustained community power is what determines whether it stays changed and whether the next tech product is deployed with the same harms.

Ways to build power:

- **Create cross-sector coalitions:** Build coalitions across technology, civil rights, journalism, law, academia, policy, and community organizing so that evidence of harm can move quickly from documentation to policy and design change demands.
- **Build a bench of Black technologists and experts:** Invest in and work with Black technologists, researchers, academics, lawyers, policy experts, and other professionals who can bring expertise from different sectors into technology accountability efforts.
- **Leverage local authority and voices:** Work through trusted local institutions — including community organizations, local elected officials, state and local regulators, educators, faith and civic leaders, and other community institutions — to elevate concerns and build pressure for changes to technology systems.

POWER PRINCIPLE

Sustained community power determines whether design changes stick and whether the next tech product is deployed with the same harms.

R.I.S.E.

Propaganda storms threaten racial inclusive democracy at the infrastructure level. These are the specific demands worth carrying into every room with the power to act.

R

REGULATORY & LEGISLATIVE ACTION

Shift accountability upstream. Safeguards on design choices, business practices, and systems that enable harmful content.

I

INVESTIGATIONS & ENFORCEMENT

Strong laws mean little without enforcement. State attorneys general, private litigation, research and watchdog efforts.

S

STRATEGIC CORPORATE ACCOUNTABILITY

Turn documented harms into targeted pressure. Mobilize advertisers. Build collective economic pressure. Target specific corporate decisions.

E

EMPOWERING COMMUNITIES

Sustained community power determines whether design changes stick. Cross-sector coalitions, Black technologists, local authority.

R.I.S.E.

Legislation and enforcement can force a company to change a design choice. **Sustained community power is what determines whether it stays changed** and whether the next tech product is deployed with the same harms.

STRUCTURAL ACTION

The same tactics can operate together at scale. Organizations can respond by documenting harm, building durable relationships, and strengthening community-controlled information infrastructure.

During this cycle

Push candidates, state officials, election administrators, and organizations toward four concrete commitments.

- First, classify coordinated digital disinformation targeting Black voters as a form of voter suppression under state law and direct state attorneys general to investigate and prosecute it. The DOJ's prior [criminal prosecution](#) in 2021 of a man who used social media to target Black voters with disinformation shows that online deception can be treated as a form of online voter suppression.
- Second, place safeguards on the use of AI in elections whether through prohibitions on deceptive synthetic media or disclosure requirements for AI-generated content.
- Third, encourage the funding of local Black press outlets and trusted community information networks as essential election infrastructure.
- Fourth, establish rapid response protocols between state election officials and community organizations so that disinformation targeting precincts triggers an immediate but thoughtful response.

BUILD THE NETWORK BEFORE THE CRISIS

The structural fight expands.

- Push for federal legislation that treats racially targeted algorithmic suppression as a civil rights violation with private right of action, meaning affected communities can sue, not just petition.
- Support development of community-controlled information infrastructure: Black-owned platforms, Black press sustainability funds, and shared verification networks that do not depend on the goodwill of the same platforms running the disinformation.

STRUCTURAL PRIORITIES

- Classify digital disinformation as voter suppression
- Safeguards on AI in elections
- Fund local Black press
- Rapid response protocols

LONG-TERM PRIORITIES

Community-controlled information infrastructure that does not depend on the same platforms running the disinformation.

Communities that face recurring propaganda storms can start now: establish relationships, build resilience networks, strengthen digital trust, and create durable ways to reach people directly.



QUICK RESOURCES

BUILD YOUR DIGITAL TRUST MAP

Are you actually reaching your community? Do you know which voices they trust, and where your network is weakest? This map answers all three questions, then hands you one clear move to build the reach you're missing.

[LINK HERE](#)



No phone handy, or want to work offline?
Download a copy you can fill out with no internet

[Click Here](#)

BREATHE. YOU ARE NOT ALONE.

You already have a plan. Work it one step at a time.

First, tell one person.

Org / Individual / Journalist

[Democracy Protection Network](#)

[Coalition Against Online Violence](#)

Voter threat

Election Protection 1-866-OUR-VOTE

Physical danger

Beacon [beacon.us](#)

Step 1 **STOP** Don't share it yet.

Ask yourself three things. If even one answer gives you pause, hold off on sharing with your wider network.

- ☐ Can I find the original source myself?
- ☐ Does it hit my feelings before it gives me facts?
- ☐ Who benefits from this spreading right now?

Step 2 **CHECK** Prove it before you move it.

A few minutes of checking beats a day of cleanup.

- ☐ Video: verify it with InVID · WeVerify
- ☐ Images: reverse-search with Google Reverse Image Search · TinEye
- ☐ Match the claim to a primary source: an official site, a named reporter, an on-the-record statement.

Step 3 **MOVE** Carry the truth on channels you own.

Once it clears, speed and repetition win.

- ☐ If almost no one has seen it, correct quietly to your closest circle instead of broadcasting.
- ☐ Send the verified story to your validators, press contacts, and email list.
- ☐ Lead with the truth and repeat the truth. Say the fact, not the false claim.
- ☐ Screenshot and document everything with timestamps as you go.

Already shared it before checking? Post one clear correction, then let it go. Correcting fast is the work.

If it is about where, when, or how to vote, move fastest. A wrong polling place or deadline may cost someone their vote. Verify only with your state Board of Elections and Election Protection at 1-866-OUR-VOTE, then move it now.

The middle of a crisis is the worst time to make a plan. You already have one. Follow it, breathe, and move one step at a time.



THE PROPAGANDA PLAYBOOK

PROPAGANDAPLAYBOOK.ORG

