The Financialization of Lawfare: Weaponizing Anti-Money Laundering Regulations and Tax Codes Against Civil Society

Executive Overview

The architecture of global financial regulation has undergone a profound structural transformation over the past two decades, evolving from a framework designed primarily to track sovereign illicit finance into a decentralized, highly automated mechanism for geopolitical and ideological enforcement. This exhaustive forensic analysis examines the systemic coordination between network-aligned legal institutes, national security think tanks, and regulatory technology (RegTech) providers to weaponize the United States Department of the Treasury's Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN). By leveraging anti-money laundering (AML) and countering the financing of terrorism (CFT) regulations, these entities effectively execute financial lawfare against domestic dissidents, anti-war advocates, and international civil liberties organizations.

This report traces the specific methodologies through which non-state proxy organizations—such as the Zachor Legal Institute and Shurat HaDin—submit formal petitions to the Treasury Department to secure Specially Designated National (SDN) and Specially Designated Global Terrorist (SDGT) classifications against targeted non-profits. The analysis further investigates the parallel legislative weaponization of Internal Revenue Code (IRC) Section 501(p). Through proposed legislation like H.R. 6408 and H.R. 9495, the executive branch seeks the unilateral authority to suspend the tax-exempt statuses of domestic charities based on classified intelligence, bypassing traditional judicial discovery, *ex parte*, and *in camera* proceedings.

Furthermore, this document maps the complex transmission mechanisms through which ideological advocacy is laundered into objective "compliance risk." White-label compliance briefs and risk advisories generated by think tanks—most notably the Foundation for Defense of Democracies (FDD) and its Center on Economic and Financial Power (CEFP)—are seamlessly integrated into the algorithmic screening tools of major global clearing banks, including JPMorgan Chase and Citibank. Powered by advanced federated machine learning platforms like Consilient and open-source intelligence engines like Giant Oak Search Technology (GOST), these compliance frameworks trigger automated, industry-wide account terminations, a phenomenon known as "de-risking". Finally, the report exposes the underlying financial and data surveillance apparatus, detailing how entities like the Vine & Fig Tree Institute fund the creation of proprietary Large Language Models (LLMs) and "Truth Databases" to monitor, aggregate, and target the digital footprint of civil society actors.

The Architecture of Financial Lawfare: Structural

Vulnerabilities in Civil Society

To understand the efficacy of financial lawfare, one must first examine the structural vulnerabilities of the modern non-profit sector and the inherent risk aversion of the global banking industry. "Lawfare" is broadly defined as the use of legal systems and regulatory frameworks as a substitute for traditional military or kinetic action to achieve operational objectives. In the financial domain, this strategy targets the circulatory system of civil society: correspondent banking relationships, payment processors, and tax-deductible philanthropy.

The "Great De-Risking" Phenomenon

Financial institutions operate under intense regulatory scrutiny. Following the expansion of the post-9/11 AML/CFT regime, clearing banks face the constant threat of multi-billion-dollar fines, deferred prosecution agreements, and severe reputational damage for facilitating illicit finance. For example, in 2011, JPMorgan Chase paid an $88 million settlement for apparent violations of OFAC sanctions programs, a relatively minor fine that nonetheless fundamentally altered the institution's internal risk calculus.

Because maintaining compliance for high-risk accounts requires extensive enhanced due diligence (EDD) and vast allocations of regulatory capital, the profitability of maintaining accounts for non-governmental organizations (NGOs) and money services businesses operating in complex geopolitical environments is severely diminished. Consequently, banks engage in systemic "de-risking"—the wholesale termination of client relationships that present elevated compliance burdens, regardless of whether the specific client has committed a crime.

Network-aligned legal groups and think tanks explicitly exploit this corporate risk aversion. By manufacturing the perception of AML/CFT risk around specific domestic and international non-profits, these actors force financial institutions to act as private censors. The banks, forced to choose between the marginal revenue of a non-profit account and the catastrophic risk of an OFAC violation, universally opt to terminate the account. This mechanism ensures that dissenting organizations are financially paralyzed without the state having to satisfy the stringent evidentiary burdens of a criminal prosecution.

Non-State Intelligence Proxies: The Orchestration of OFAC and FinCEN Designations

The tip of the spear in modern financial lawfare is the targeted petitioning of the Treasury Department. By acting as non-state intelligence proxies, specialized legal institutes aggregate open-source data, financial records, and ideological statements, repackaging them into formal complaints that trigger devastating regulatory actions.

Shurat HaDin and the Doctrine of Preemptive Financial Liability

Operating in close coordination with Israeli state intelligence apparatuses—including the Ministry of Strategic Affairs—Shurat HaDin (the Israel Law Center) has pioneered the doctrine of preemptive financial liability. Shurat HaDin’s operational methodology, often referred to as the "Harpoon" doctrine, focuses explicitly on dismantling the financial infrastructure of perceived adversaries through the threat of civil litigation and regulatory exposure.

The organization’s tactics are multifaceted but rely primarily on placing financial and logistical institutions "on notice" regarding potential violations of the United States Anti-Terrorism Act. By issuing formal legal warnings to banks, insurance companies, and clearinghouses, Shurat HaDin shifts the legal liability directly onto the corporate entity.

A prime illustration of this tactic occurred during the organization of maritime flotillas attempting to breach blockades. Shurat HaDin systematically identified the maritime insurance companies underwriting the vessels and issued formal letters warning that insuring such boats exposed the insurers to charges of materially supporting terrorism, making them civilly liable for any future kinetic attacks. Faced with this unquantifiable liability, insurers like Inmarsat preemptively terminated satellite communication services and insurance coverage, effectively grounding the vessels without direct state intervention.

In the domestic and European banking sectors, this strategy is equally devastating. In 2019, the German SozialBank (Bank für Sozialwirtschaft) summarily shut down the account of the Jewish Voice for a Just Peace—a local organization advocating for Palestinian rights—after Shurat HaDin submitted a formal letter alleging the group had ties to terrorism and warning the bank of its exposure to U.S. criminal and civil liability. Similarly, the digital fundraising platform Donorbox suspended the accounts of groups associated with boycott movements following coordinated complaints from Shurat HaDin and the Israeli government, explicitly citing the need to "review evidence" as a precautionary compliance measure.

The Zachor Legal Institute’s Coordinated Campaign for SDN Classifications

While Shurat HaDin focuses on civil liability and direct corporate pressure, the Zachor Legal Institute represents the primary domestic vector for securing formal Treasury designations. Led by Marc Greendorfer, Zachor produces extensive legal scholarship and submits formal, highly detailed petitions to OFAC and FinCEN, arguing that specific civil liberties organizations, anti-war groups, and humanitarian NGOs function as front organizations for designated foreign terrorist organizations (FTOs) such as Hamas and the Popular Front for the Liberation of Palestine (PFLP).

Zachor’s operations are highly coordinated and synchronized with the political climate. In a detailed, eight-page memorandum forwarded to senior Republican staffers on the House Foreign Affairs and Ways and Means committees in November 2023, Zachor alleged that designated terrorist groups were exploiting "little-known loopholes" in the U.S. financial system to evade OFAC sanctions by enlisting third-party domestic charities as support organs.

This legislative lobbying laid the groundwork for targeted administrative action. Zachor's most significant regulatory victory occurred in October 2024, when OFAC—acting in concert with the Canadian government—officially designated the Samidoun Palestinian Prisoner Solidarity Network as a Specially Designated Global Terrorist (SDGT) and added it to the SDN list. OFAC justified the designation by categorizing Samidoun as a "sham charity" acting as an international fundraiser for the PFLP. This designation instantly froze all of Samidoun's assets under U.S. jurisdiction and imposed secondary sanctions risks—pursuant to Executive Order 13224—on any financial institution globally that facilitated transactions on its behalf.

Tracing the Designation Cascade: From Samidoun to the Alliance for Global Justice

The designation of Samidoun triggered a pre-planned cascade of financial de-risking that successfully crippled its domestic fiscal sponsor, the Alliance for Global Justice (AfGJ). AfGJ is an Arizona-based 501(c)(3) non-profit that acts as a fiscal umbrella for over 140 grassroots economic, social justice, and human rights projects globally that lack their own tax-exempt infrastructure.

Because AfGJ processed donations for Samidoun, the OFAC designation of the latter was immediately weaponized against the former. Following formal IRS complaints submitted by the Zachor Legal Institute and highly coordinated media pressure campaigns highlighting the FTO linkages, major financial service providers severed ties with AfGJ. In rapid succession, payment processors including Discover, Stripe, Salsa Labs, and PayPal terminated AfGJ's ability to process credit card transactions. This collateral damage is a hallmark of financial lawfare: by targeting a single node (Samidoun), the attackers successfully de-platformed an entire network of 140 disparate civil society organizations that relied on AfGJ's financial infrastructure.

Emboldened by the success of the Samidoun/AfGJ operation, Zachor Legal Institute rapidly expanded its targeting matrix. In February and March 2025, Zachor led a coalition of 45 organizations in submitting a comprehensive petition to newly appointed Treasury Secretary Scott Bessent, demanding that OFAC issue SDN designations against six additional NGOs. These organizations included Addameer (Prisoner Support and Human Rights Association), the Bisan Center for Research and Development, the Al-Haq Organization, Defense for Children International – Palestine (DCI-P), the Union of Palestinian Women's Committees (UPWC), and the Union of Agricultural Work Committees (UAWC). Zachor argued that failing to designate these entities would simply allow Samidoun's illicit activities to be absorbed by other non-SDN entities. The mere filing of this petition resulted in immediate structural damage; following the request, domains and social media presences associated with Addameer were taken down by hosting providers fearful of secondary sanctions exposure.

Targeted Entity	Lawfare Vector / Petitioner	Regulatory / Corporate Consequence	Broader Systemic Impact	Source
Samidoun	OFAC Petition via Zachor Legal Institute	Designated as SDN/SDGT; assets frozen globally.	Established the legal and regulatory precedent to target domestic fiscal sponsors.	
Alliance for Global Justice (AfGJ)	IRS Complaints; Media Pressure Campaigns	Loss of Stripe, PayPal, Discover, and Salsa Labs.	Financial paralysis of over 140 affiliated civil society and human rights projects.	
Addameer, Bisan, Al-Haq, DCI-P	Coordinated OFAC Petition by 45-group coalition	Extreme sanctions risk; web domains removed by hosts.	Severe degradation of international human rights monitoring and humanitarian aid operations.	
Jewish Voice for	Direct Warning	Account	Demonstrated the	

Targeted Entity	Lawfare Vector / Petitioner	Regulatory / Corporate Consequence	Broader Systemic Impact	Source
a Just Peace	Letter via Shurat HaDin	unilaterally terminated by German SozialBank.	efficacy of utilizing the U.S. Anti-Terrorism Act to compel European bank compliance.	

The Weaponization of the Internal Revenue Code: Section 501(p) and the Eradication of Due Process

While OFAC designations represent a potent tool for international disruption, the regulation of domestic non-profits is primarily governed by the Internal Revenue Service (IRS). Traditionally, the revocation of a domestic organization's 501(c)(3) tax-exempt status requires a rigorous, case-by-case IRS audit, affording the entity ample opportunity to defend itself through multiple routes of administrative and judicial appeal. Furthermore, criminal prosecution for providing "material support for terrorism" under 18 U.S.C. § 2339B requires the government to meet high evidentiary standards, providing the accused with discovery and constitutional due process. However, recent administrative maneuvers and aggressive legislative proposals seek to bypass these protections entirely, weaponizing the Internal Revenue Code to unilaterally dismantle targeted civil liberties organizations.

The Mechanics of IRC Section 501(p)

Enacted in 2003 during the post-9/11 expansion of executive power, Internal Revenue Code Section 501(p) provides a narrow but devastating exception to standard IRS procedures. Under Section 501(p), if the federal government designates an organization as a terrorist entity—typically via an Executive Order under the International Emergency Economic Powers Act (IEEPA) or the Immigration and Nationality Act (INA)—the IRS is mandated to automatically suspend the organization's tax-exempt status.

The operational mechanics of Section 501(p) are explicitly designed to circumvent due process. The suspension is immediate; the IRS has zero administrative discretion and provides no advance notice or pre-deprivation hearing. The consequences are instant and catastrophic: the organization loses its recognition under Section 501(a), contributions made by donors are no longer tax-deductible, and private philanthropic foundations are legally prohibited from making qualifying distributions or grants to the targeted entity. Crucially, the organization cannot appeal the suspension directly to the IRS; relief can only be obtained if the originating national security agency (e.g., OFAC or the State Department) lifts the underlying terrorism designation.

Legislative Escalation: H.R. 6408 and H.R. 9495

Recognizing the administrative efficiency of Section 501(p), network-aligned legislative efforts—specifically H.R. 6408 and its revived iteration, H.R. 9495 (the "Stop Terror-Financing and Tax Penalties on American Hostages Act")—have sought to drastically expand the Treasury Secretary's unilateral authority.

These legislative proposals introduce a profoundly expansive legal category: the "terrorist supporting organization". Rather than requiring an organization to be formally designated as a primary terrorist entity, H.R. 9495 grants the Secretary of the Treasury the power to strip a U.S. non-profit of its tax-exempt status if the Secretary determines the entity provided "material support or resources" to a terrorist group within the preceding three-year period.

The systemic implications of this shift have alarmed a broad spectrum of civil society. Organizations ranging from the ACLU to the NAACP have decried the provision, arguing that it conflates strict criminal law standards with arbitrary tax code enforcement. By granting the executive branch the unilateral authority to interpret what constitutes "material support" without the burden of criminal proof, the legislation creates a framework inherently susceptible to politicized misuse, allowing administrations to financially starve political opponents, civil rights groups, and dissenting activist networks under the guise of national security.

Bypassing Judicial Discovery: Ex Parte and In Camera Proceedings

The most legally consequential and structurally dangerous element of H.R. 9495 is its explicit circumvention of judicial transparency and discovery. Under standard constitutional frameworks, an organization accused of facilitating illicit activity possesses the right to examine the evidence against it, cross-examine witnesses, and mount a robust defense. H.R. 9495 systematically dismantles this right.

The legislation outlines a highly constrained review process. Upon receiving notice of a pending designation, a non-profit is granted a 90-day window to satisfy the Treasury Secretary that it did not provide material support, or that it has made reasonable efforts to halt such support. While the organization may seek administrative review through the IRS Independent Office of Appeals, the legislation explicitly states that a designation remains final even if the organization fails to utilize this internal dispute resolution process.

If the targeted non-profit seeks judicial review in a U.S. district court, it confronts an insurmountable procedural barrier. H.R. 9495 stipulates that if the Treasury's determination is based on classified information—as defined in Section 1(a) of the Classified Information Procedures Act (CIPA)—that intelligence may be submitted to the reviewing court *ex parte* and *in camera*.

In practice, this means the presiding judge reviews the government's evidence in absolute secrecy. The targeted domestic non-profit, its board of directors, and its legal counsel are strictly prohibited from viewing the underlying intelligence, the sources of the information, or the methodologies used to secure the designation. Consequently, domestic charities are denied the fundamental right to confront their accusers. A legal standard previously reserved for foreign espionage, treason, or high-level counter-terrorism operations is thereby transposed onto the regulation of domestic 501(c)(3) advocacy groups, ensuring that the financial execution of the organization occurs before any public adjudication of the facts can take place.

Legal Framework	Evidentiary Standard	Due Process / Discovery Rights	Judicial Review Mechanism	Impact on Civil Society
Traditional Criminal Prosecution (18 U.S.C. § 2339B)	Beyond a reasonable doubt; explicit proof of knowing material support.	Full constitutional discovery; right to confront evidence and cross-examine.	Public trial by jury in federal court.	High threshold prevents arbitrary politicized targeting.
Traditional IRS	Preponderance of	Advance notice;	U.S. Tax Court or	Procedural

Legal Framework	Evidentiary Standard	Due Process / Discovery Rights	Judicial Review Mechanism	Impact on Civil Society
Revocation	evidence of substantial non-exempt activity.	multi-level audit; robust administrative appeals.	federal district court with full discovery.	safeguards protect against sudden financial ruin.
Current IRC Section 501(p)	Automatic trigger based on formal IEEPA/INA designation.	Zero advance notice; zero pre-deprivation hearing.	None at the IRS level; must challenge underlying Executive Order.	Immediate loss of funding; highly disruptive but historically limited scope.
Proposed Expansion (H.R. 9495)	Unilateral Treasury determination of "material support" (3-year lookback).	90-day administrative cure period; **no right to access classified evidence.**	U.S. district court review utilizing ***ex parte*** **and** ***in camera*** secret evidence.	Weaponizes tax code; allows executive branch to secretly dismantle domestic dissenting groups.

The Intellectual Vanguard: Think Tanks, White-Label Compliance, and Risk Standardization

While OFAC petitions and 501(p) suspensions represent the sharp, visible edge of financial lawfare, the broader efficacy of this strategy relies on the subtle, systemic manipulation of the global banking sector's internal compliance infrastructure. This translation of ideological policy into corporate procedure is facilitated by prominent national security think tanks, which act as critical intermediaries between aggressive policy advocates and risk-averse financial institutions.

The Foundation for Defense of Democracies (FDD) and the CEFP

The Foundation for Defense of Democracies (FDD) and its Center on Economic and Financial Power (CEFP) operate as the intellectual command center for modern economic statecraft. Unlike traditional academic institutions, the FDD is uniquely structured to influence financial regulation, heavily populated by former high-ranking Treasury and national security officials who architected the post-9/11 financial warfare regime.

Key personnel within the CEFP include Juan Zarate, the first-ever Assistant Secretary of the Treasury for Terrorist Financing and Financial Crimes; Daniel Glaser, former Assistant Secretary for Terrorist Financing; and Elaine Dezenski, a former senior official at the Department of Homeland Security. By leveraging their deep institutional knowledge and extensive networks within both the regulatory state and the private sector, these figures exert unparalleled influence over how AML/CFT regulations are interpreted and enforced.

The FDD routinely submits extensive commentaries to FinCEN regarding proposed rulemakings. In these submissions, the FDD consistently advocates for a shift away from procedural "box-checking" toward an "effectiveness-based, risk-calibrated" compliance framework. While ostensibly designed to reduce unnecessary bureaucratic burdens, this effectiveness standard empowers financial institutions to aggressively de-risk specific sectors based on targeted intelligence. The FDD argues that modern adversaries—including sanctioned

state actors and terrorist proxies—do not collapse entire AML programs; rather, they exploit single gaps at single institutions. This narrative demands that banks implement hyper-vigilant, targeted screening of NGOs and international payment networks, aligning corporate compliance directly with the FDD's geopolitical threat matrices.

The Propagation of White-Label Compliance Briefs

To ensure that their specific policy objectives and target lists are adopted by the private sector, think tanks like the FDD generate extensive risk advisories, policy memorandums, and "white-label" compliance briefs.

In the financial industry, "white-label" refers to a product or service produced by one entity but utilized by another as if it were their own. White-label compliance infrastructure is common in sectors ranging from independent ATMs to stablecoin issuance, allowing banks to outsource complex risk assessments to specialized third parties. Think tanks exploit this reliance by producing highly detailed compliance briefs that map out specific typologies of illicit finance. These briefs identify high-risk geographic regions, outline the operational structures of suspected proxy organizations, and highlight specific transaction patterns associated with sanctioned actors.

Because global clearing banks—such as JPMorgan Chase and Citibank—handle trillions of dollars in daily transfer volume, they are inherently terrified of regulatory failure. They eagerly ingest these white-label compliance briefs from highly credentialed think tanks, utilizing them as a pre-packaged regulatory shield. By adopting the risk parameters defined by former Treasury officials at the FDD, a bank can demonstrate to FinCEN examiners that its AML program utilizes "industry-leading" intelligence and proactive risk mitigation.

However, a profound systemic consequence emerges from this reliance: when an ideological think tank defines the risk parameters, it inherently embeds its own geopolitical biases into the banking sector's supposedly neutral compliance algorithms. If an FDD policy memorandum associates a specific humanitarian corridor in the Middle East or a domestic anti-war advocacy network with "high sanctions evasion risk," the clearing bank will inevitably adjust its transaction monitoring systems to flag any financial activity matching those profiles. This effectively privatizes the enforcement of foreign policy, allowing think tanks to dictate which organizations maintain access to the global financial system without requiring a formal act of Congress or a Treasury designation.

Technological Execution: RegTech, Federated AI, and Automated De-Risking

The transition of a think tank's risk advisory into the actual termination of an NGO's bank account is rarely a manual, human-driven process. The sheer volume of global financial transactions necessitates that AML screening be heavily automated. Consequently, specialized regulatory technology (RegTech) providers and private intelligence firms serve as the mechanical executioners of financial lawfare, translating subjective policy papers into objective algorithmic triggers.

K2 Integrity, Consilient, and Federated Machine Learning

The seamless integration of policy advocacy and technological execution is epitomized by Juan

Zarate. In addition to his role at the FDD, Zarate serves as the Global Co-Managing Partner and Chief Strategy Officer at K2 Integrity, a premier global risk and compliance consultancy that advises Tier 1 banks on AML/CFT remediation. Furthermore, Zarate is the co-founder and Chair of the Board of Consilient, an innovative FinTech company dedicated to establishing the next-generation AML/CFT system.

Consilient introduces a revolutionary—and highly consequential—approach to financial crime detection through the application of "federated machine learning". Historically, financial institutions operated in silos, unable to share comprehensive data regarding illicit finance due to strict privacy laws, competitive burdens, and technological fragmentation. Consilient's flagship Dozer™ technology platform circumvents these obstacles by sharing the algorithmic models themselves, rather than the underlying customer data, across multiple financial institutions. Utilizing Intel's Software Guard Extensions (Intel® SGX) for confidential computing, Consilient trains its algorithms on isolated datasets and then distributes the refined risk-detection model globally.

While federated learning is marketed as a tool to drastically reduce false positives (reportedly from above 90% down to 12%) and increase efficiency, its systemic impact is profound: it effectively synchronizes the risk appetite of the entire global banking sector. If a federated machine learning model is trained on risk parameters derived from network-aligned OFAC petitions and FDD compliance briefs, a single domestic NGO flagged by the algorithm will find itself systematically targeted by every major bank simultaneously. The organization is not merely rejected by one institution; it is locked out of the entire interconnected financial ecosystem through a universally shared algorithmic consensus.

Giant Oak Search Technology (GOST)

The mechanism of targeting relies deeply on continuous, automated open-source intelligence (OSINT) gathering. Consilient was launched in collaboration with Gary M. Shiffman, the founder and CEO of Giant Oak. Giant Oak's primary product, Giant Oak Search Technology (GOST), is an open-source search and triage tool explicitly designed to detect suspicious behavior and combat financial crime.

GOST operates by building customized internet domains and continuously re-indexing the open and deep web to retrieve publicly available electronic information (PAEI). Utilizing advanced machine-learning algorithms, GOST refines search results, generates analytic risk scores, and sorts entities by relevance and threat level. This tool is deeply integrated into the Client Due Diligence (CDD) and continuous Know Your Customer (KYC) workflows of financial institutions.

The integration of GOST completes the weaponization loop. When an advocacy group like the Zachor Legal Institute submits a highly publicized OFAC petition, or when a media outlet publishes a derogatory report alleging an NGO has ties to a designated FTO, GOST instantly ingests these digital artifacts. The algorithm assigns a high-risk analytic score to the targeted NGO and automatically pushes this flag to the compliance dashboards of clearing banks.

The Mechanics of the De-Risking Cascade

Once the automated systems (powered by Consilient's federated models and GOST's OSINT triage) flag a non-profit organization as a potential AML/CFT vulnerability, the bank initiates the de-risking process. This involves the immediate generation of a Suspicious Activity Report (SAR) and the unilateral termination of the client relationship.

Because the algorithms target the central nodes of the financial system, the cascading effects

are devastating. The breakdown of correspondent banking relationships means the targeted organization loses access to essential financial infrastructure: payment processors like Stripe and PayPal freeze funds, payroll providers refuse to process employee salaries, and international wire transfers to humanitarian aid projects are permanently blocked. The organization is financially eradicated, not by the ruling of a judge, but by an automated algorithmic determination that managing their account presents an unacceptable regulatory burden to the bank.

The Dark Money Data Surveillance Apparatus: Vine & Fig Tree and Algorithmic Lawfare

The immense volume of intelligence required to feed OFAC petitions, generate think tank compliance briefs, and manipulate the algorithms of GOST demands massive, sustained financial backing and sophisticated surveillance capabilities. This ecosystem is financed and operated by a highly opaque network of philanthropic funds and specialized technological platforms.

The Financial Engine: Vine & Fig Tree

The Vine & Fig Tree Institute (and its grantmaking arm, the Vine & Fig Tree Fund) operates as a primary financial node within this lawfare network. With a stated public mission to combat antisemitism, promote tolerance, and accelerate civic cohesion, the organization deploys millions of dollars annually to a highly interconnected web of affiliated projects and advocacy groups.

A significant and consistent beneficiary of Vine & Fig Tree's capital is the Combat Hate Foundation, the 501(c)(3) entity that operates the Combat Antisemitism Movement (CAM). Financial disclosures reveal that Vine & Fig Tree regularly provides substantial six-figure grants to the Combat Hate Foundation, as well as to allied organizations such as the Philos Project and the Giving Back Fund.

These funds directly subsidize the ideological and operational infrastructure required to identify, monitor, and build cases against targeted civil society groups. CAM, under the direction of figures like Mikhail Galperin and Adam Beren, acts as a central coordinating hub, collaborating closely with legal actors such as the Zachor Legal Institute to apply pressure on academic institutions, local governments, and federal agencies regarding the activities of domestic activist networks and pro-Palestinian advocacy groups.

The "Truth Database" and the Automation of Surveillance

Beyond traditional grantmaking and policy advocacy, Vine & Fig Tree invests heavily in the development of advanced technological capabilities to automate its surveillance and targeting objectives. Notably, recent financial disclosures from the UJA-Federation of New York document a $200,000 grant directed to the Vine & Fig Tree Institute explicitly for the development of a "Truth Database and Large Language Model (LLM)".

The funding and deployment of proprietary LLMs and centralized intelligence databases represents a quantum leap in the industrialization of lawfare. Organizations like CAM have launched highly sophisticated digital portals, such as the "Report It" application, designed to crowd-source and aggregate accusations of ideological dissent, hate speech, and boycott

advocacy across major social media platforms, including Facebook, Instagram, TikTok, and YouTube. This raw, crowd-sourced data is systematically documented and stored in secure, centralized online databases.

Concurrently, CAM's Antisemitism Research Center actively monitors and analyzes AI-generated misinformation networks, demonstrating a deep organizational fluency in the mechanics of algorithmic narrative control. By aggregating massive volumes of behavioral, financial, and rhetorical data through these LLM-powered databases, network actors can generate highly detailed, automated dossiers on domestic non-profits, student groups, and international NGOs.

These comprehensive dossiers are subsequently reformatted into the formal legal complaints submitted to OFAC and FinCEN by organizations like Zachor, or they are amplified through coordinated media channels to ensure they are captured by the RegTech screening tools (like GOST) utilized by major clearing banks. It is a flawlessly engineered, self-sustaining cycle: proprietary LLMs aggregate the target data, legal proxies file the administrative complaints, think tanks define the compliance risk, and banking algorithms execute the financial exclusion.

Component	Key Actors & Technologies	Function within the Lawfare Ecosystem	Source
Financial Engine	Vine & Fig Tree Fund; Donor Advised Funds	Deploys millions in dark money to subsidize the operational and technological costs of surveillance and advocacy groups.	
Surveillance & Data Aggregation	Combat Antisemitism Movement (CAM); "Truth Database"; LLMs; "Report It" App	Crowd-sources, scrapes, and analyzes digital footprints to build comprehensive targeting dossiers on civil society actors.	
Legal/Regulatory Targeting	Zachor Legal Institute; Shurat HaDin	Converts surveillance dossiers into formal OFAC petitions, IRS complaints, and threats of Anti-Terrorism Act civil liability.	
Algorithmic Execution	FDD (Risk Briefs); Consilient (Federated AI); GOST	Ingests the regulatory complaints and translates them into automated CDD/KYC flags, triggering universal banking de-risking.	

Systemic Impacts and the Future of Civil Society

The forensic mapping of this ecosystem reveals that the suppression of domestic dissidents, anti-war advocates, and international civil liberties organizations is no longer reliant on the overt mechanisms of state censorship or the protracted, high-burden processes of criminal trials.

Instead, the architecture of control has been seamlessly integrated into the frictionless, automated plumbing of the global financial system.

The systemic coordination between non-state intelligence proxies (Zachor Legal Institute, Shurat HaDin), intellectual validators (FDD, CEFP), and technological executioners (K2 Integrity, Consilient, GOST) has successfully outsourced the policing of ideological boundaries to the compliance departments of commercial banks. By leveraging OFAC petitions to trigger algorithmic de-risking, this network has engineered a nearly impenetrable matrix of financial exclusion.

Simultaneously, the aggressive legislative push to expand Internal Revenue Code Section 501(p) through bills like H.R. 9495 threatens to permanently sever the fundamental constitutional protections of domestic 501(c)(3) organizations. By granting the executive branch the unilateral authority to interpret "material support," and by explicitly allowing the use of classified intelligence in *ex parte* and *in camera* judicial proceedings, the state can financially dismantle political opponents and dissenting activist networks in absolute secrecy, denying them the right to discovery or a fair defense.

The convergence of opaque tax laws, highly sensitive banking compliance algorithms, and AI-driven data surveillance represents an existential threat to the operational viability of civil society. Because financial institutions will always prioritize existential regulatory compliance over the preservation of marginal non-profit accounts, the privatization of censorship is complete. Without urgent structural interventions—including the establishment of clear safe harbors for legitimate humanitarian activity, the enforcement of rigorous evidentiary standards before tax exemptions are suspended, and the protection of constitutional discovery rights against the use of secret evidence—the architecture of financial lawfare will continue to expand. It will operate silently and algorithmically to neutralize targeted advocacy, starving civil society of the resources it needs to exist before a single legal argument can ever be heard in open court.

Works cited

1. 2023–2024 judicial aiding and abetting 589 judicial aiding and abetting of terror marc a. greendorfer - Boston University, https://www.bu.edu/rbfl/files/2025/02/GREENDORFER-MACHOL.pdf 2. Report of the Attorney General to the Congress of the United States on the Administration of the Foreign Agents Registration Act - Department of Justice, https://www.justice.gov/nsd-fara/page/file/1448896/dl?inline 3. Suppressing Dissent - OAPEN Library, https://library.oapen.org/bitstream/handle/20.500.12657/95695/external_content.pdf?sequence=1&isAllowed=y 4. Hamas: Background & Overview - Jewish Virtual Library, https://jewishvirtuallibrary.org/background-and-overview-of-hamas 5. Sanctions List Search - OFAC, https://sanctionssearch.ofac.treas.gov/Details.aspx?id=47582 6. Counter Terrorism Designations | Office of Foreign Assets Control, https://ofac.treasury.gov/recent-actions/20241015 7. ACLU letter urging Congress to oppose H.R. 6408/S. 4136 | American Civil Liberties Union, https://www.aclu.org/documents/aclu-letter-urging-congress-to-oppose-h-r-6408-s-4136 8. Congressional Record, Volume 170 Issue 173 (Thursday, November 21, 2024) - GovInfo, https://www.govinfo.gov/content/pkg/CREC-2024-11-21/html/CREC-2024-11-21-pt1-PgH6159-3.htm 9. HR 9495 and its Implications for Nonprofit Organizations - Apex Law Group, https://apexlg.com/hr-9495-and-its-implications-for-nonprofit-organizations/ 10. House Report 118-729 - STOP TERROR-FINANCING AND TAX PENALTIES ON AMERICAN HOSTAGES

ACT - GovInfo,
https://www.govinfo.gov/content/pkg/CRPT-118hrpt729/html/CRPT-118hrpt729.htm 11. Mandates of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism - ohchr,
https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=29696 12. What 111 Industry Voices Told FinCEN About the Future of AML - Blog | Unit21,
https://www.unit21.ai/blog/what-111-industry-voices-told-fincen-about-the-future-of-aml 13. Anti-Money Laundering and Countering the Financing of Terrorism Programs - FDD,
https://www.fdd.org/analysis/2026/06/08/anti-money-laundering-and-countering-the-financing-of-terrorism-programs/ 14. A Gameplan for American Economic Security - FDD,
https://www.fdd.org/events/2026/05/05/a-gameplan-for-american-economic-security/ 15. Elaine K. Dezenski,
https://docs.house.gov/meetings/FA/FA05/20250514/118242/HHRG-119-FA05-Bio-DezenskiE-20250514-U1.pdf 16. Consilient Bank Trials Demonstrate Federated Machine Learning Improves Effectiveness And Efficiency For Financial Crime Detection - K2 Integrity,
https://www.k2integrity.com/en/newsroom/news-releases/consilient-bank-trials-demonstrate-technologys-effectiveness-for-banks/ 17. Consilient: K2 Intelligence Financial Integrity Network and Giant Oak Collaborate with Intel to Launch the New Approach to Fighting Financial Crime,
https://consilient.com/consilient-k2-intelligence-financial-integrity-network-and-giant-oak-collaborate-with-intel-to-launch-the-new-approach-to-fighting-financial-crime 18. Profiles of the RegTech100, the world's most innovative RegTech companies that every leader in the regulatory industry needs t - FinTech Global,
https://fintech.global/regtech100/wp-content/uploads/2019/12/RegTech100_2020_Summary.pdf 19. Understanding Bank De-Risking and its Effects on Financial Inclusion: An exploratory study - Oxfam,
https://www-cdn.oxfam.org/s3fs-public/file_attachments/rr-bank-de-risking-181115-en_0.pdf 20. report of 2024-2025 - grants awarded - UJA-Federation,
https://www.ujafedny.org/api/v2/assets/Grants-Book-2025.pdf 21. Help Fight Rising Online Antisemitism With New Digital Portal 'Report It',
https://combatantisemitism.org/campaigns/help-fight-rising-online-antisemitism-with-new-digital-portal-report-it/ 22. Lawfare - Jurist Panel,
https://www.juristpanel.com/wp-content/uploads/2023/04/Orde-F.-Kittrie-Lawfare.pdf 23. The Lawyer Hamas Fears: Nitsana Darshan-Leitner - Everything-PR,
https://everything-pr.com/nitsana-darshan-leitner-shurat-hadin-lawyer-hamas-fears 24. - MANAGING TERRORISM FINANCING RISK IN REMITTANCES AND MONEY TRANSFERS - GovInfo,
https://www.govinfo.gov/content/pkg/CHRG-115hhrg29451/html/CHRG-115hhrg29451.htm 25. managing terrorism financing risk in remittances and money transfers hearing - House Committee on Financial Services, https://financialservices.house.gov/uploadedfiles/115-32.pdf 26. The Challenge Of Transparency In Preventing Financial Crime: Navigating Financial Integrity In A Changing Risk Landscape - K2 Integrity,
https://www.k2integrity.com/en/knowledge/expert-insights/2023/the-challenge-of-transparency-in-preventing-financial-crime-navigating-financial-integrity-in-a-changing-risk-landscape/ 27. Financial Warfare: Sanctions and Watchlists Disrupt Terror Funding Networks Amid International Conflict - Global RADAR,
https://globalradar.com/financial-warfare-sanctions-and-watchlists-disrupt-terror-funding-networks-amid-international-conflict/ 28. Iraq's bake sale for the Islamic Republic - FDD,
https://www.fdd.org/analysis/2026/04/07/iraqs-bake-sale-for-the-islamic-republic/ 29.

Recommendations for Regulating and Supervising Bank and Non-bank Payment Service Providers Offering Cross-border Payment Service - Financial Stability Board, https://www.fsb.org/uploads/P160724-2.pdf 30. Schedule 1 Reversion: The Looming Banking Crisis for Non-Compliant CBD Wholesalers, https://lowgravityhemp.com/blogs/news/schedule-1-reversion-the-looming-banking-crisis-for-non-compliant-cbd-wholesalers 31. US fundraising site suspends BDS account over alleged terror ties | The Times of Israel, https://www.timesofisrael.com/us-fundraising-site-suspends-bds-account-over-alleged-terror-ties/ 32. LAWFARE: TACTICS AND TECHNIQUES - National Maritime Foundation, https://maritimeindia.org/lawfare-tactics-techniques-and-case-studies/ 33. International Law and the Use of Lawfare: An Argument for the U.S. To Adopt a Lawfare Doctrine - BearWorks - Missouri State University, https://bearworks.missouristate.edu/cgi/viewcontent.cgi?article=4156&context=theses 34. Palestinian terrorists 'exploit loopholes' for taxpayer dollars, watchdog tells Congress, https://zachorlegal.org/2023/11/08/palestinian-terrorists-exploit-loopholes-taxpayer-dollars-watchdog-tells-congress/ 35. News Archives - Zachor Legal Institute, https://zachorlegal.org/category/news/ 36. Dr. Mark Goldfeder, Esq. - The Federalist Society, https://fedsoc.org/bio/mark-goldfeder 37. Treasury Sanctions Sham Charity for Terrorist Ties Following Ways and Means Investigation, https://waysandmeans.house.gov/2024/10/16/treasury-sanctions-sham-charity-for-terrorist-ties-following-ways-and-means-investigation/ 38. Government of Canada lists Samidoun as a terrorist entity, https://www.canada.ca/en/public-safety-canada/news/2024/10/government-of-canada-lists-samidoun-as-a-terrorist-entity.html 39. Chairman Smith: Ending Taxpayer Subsidies for Terrorist Organizations Shouldn't Be Hard, https://waysandmeans.house.gov/2024/11/20/chairman-smith-ending-taxpayer-subsidies-for-terrorist-organizations-shouldnt-be-hard/ 40. Alliance for Global Justice - NGO Monitor, https://ngo-monitor.org/funder/alliance-for-global-justice/ 41. Human Rights Coalition Deplatformed After Lawfare Attack - Charity & Security Network, https://charityandsecurity.org/deplatforming/human-rights-coalition-deplatformed-after-lawfare-attack/ 42. Pro-Israel Groups Urge Trump to Sanction Palestinian NGOs Out of Existence | Truthout, https://truthout.org/articles/pro-israel-groups-urge-trump-to-sanction-palestinian-ngos-out-of-existence/ 43. Coalition urges US Treasury to sanction six alleged terror-linked NGOs | The Jerusalem Post, https://www.jpost.com/diaspora/antisemitism/article-844736 44. Addameer - Wikipedia, https://en.wikipedia.org/wiki/Addameer 45. Nonprofits Under Fire: How the IRS Can – and Cannot – Revoke Federal Tax-Exempt Status, https://www.tenenbaumlegal.com/nonprofits-under-fire-how-the-irs-can-and-cannot-revoke-federal-tax-exempt-status/ 46. Evolving Threats to the Tax-Exempt Status of 501(c)(3) Nonprofits - ICNL, https://www.icnl.org/post/news/evolving-threats-to-the-tax-exempt-status-of-501c3-nonprofits 47. Revived Nonprofit Killer Bill Back in the House - MLFA, https://mlfa.org/revived-nonprofit-killer-bill-back-in-the-house/ 48. Federal Terrorism Law and U.S. Civil Society: An Explainer - ICNL, https://www.icnl.org/federal-terrorism-law-and-u-s-civil-society-an-explainer 49. TG 45: Suspension of Tax-Exempt Status of Terrorist Organizations under IRC 501(p) - IRS, https://www.irs.gov/pub/irs-pdf/p5588.pdf 50. Tax Alert: The Legal Rights of Charities to Defend Charitable Status - Shulman Rogers,

https://www.shulmanrogers.com/tax-alert-the-legal-rights-of-charities-to-defend-charitable-status / 51. Executive Orders, § 501(p), and Nonprofits - Charity Lawyer Blog, https://charitylawyerblog.com/2025/10/06/executive-orders-%C2%A7-501p-and-nonprofits/ 52. H.R. 9495: Stop Terror-Financing and Tax Penalties on American Hostages Act, https://nonprofitlawblog.com/h-r-9495-stop-terror-financing-and-tax-penalties-on-american-hostages-act/ 53. Non-Profits Targeted Under New Tax Code Proposals | Jenner & Block LLP | Law Firm, https://www.jenner.com/en/news-insights/client-alerts/non-profits-targeted-under-new-tax-code-proposals 54. Description of HR 9495, the “Stop Terror-Financing and Tax Penalties on American Hostages Act” - Ways and Means Committee, https://waysandmeans.house.gov/wp-content/uploads/2024/09/JCT-Description-of-H.R.-9495.pdf 55. House Approves Law Against Nonprofits the Support Terrorist Groups, https://www.jewishvirtuallibrary.org/house-approves-law-against-nonprofits-the-support-terrorist-groups 56. A Gameplan for American Economic Security: - FDD, https://www.fdd.org/analysis/2026/05/04/a-gameplan-for-american-economic-security-supercharging-u-s-statecraft-from-an-economic-pentagon-to-the-near-global-economy/ 57. Juan C. Zarate - K2 Integrity, https://www.k2integrity.com/en/people/professionals/zarate-c-juan/ 58. Hon. Juan C. Zarate - The Federalist Society, https://fedsoc.org/bio/juan-zarate 59. Elaine K. Dezenski - FDD, https://www.fdd.org/team/elaine-dezenski/ 60. Daniel Glaser - FDD, https://www.fdd.org/team/daniel-glaser/ 61. Maximum Support for the Iranian People: A New Strategy - FDD, https://www.fdd.org/wp-content/uploads/2022/10/fdd-memo-maximum-support-for-the-iranian-people.pdf 62. Iranian and Iranian-Backed Attacks Against Americans (1979-Present) - FDD, https://www.fdd.org/analysis/2025/06/19/iranian-and-iranian-backed-attacks-against-americans-1979-present/ 63. Exhibit - SEC.gov, https://www.sec.gov/Archives/edgar/data/1488813/000148881319000031/a1022cobaltagreementa.htm 64. White-Label Franchise Platform | Your Brand, Your OS — FranchiseLauncher, https://franchiselauncher.com/white-label 65. Federal Register/Vol. 91, No. 40/Monday, March 2, 2026/Proposed Rules - OCC.gov, https://www.occ.treas.gov/news-issuances/federal-register/2026/91fr10202.pdf 66. US Treasury anti-laundering unit urges banks to consider serving independent ATM operators - Thomson Reuters Institute, https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/treasury-aml-atms/ 67. Notice of proposed rulemaking: Implementing the Guiding and Establishing National Innovation for U.S. Stablecoins Act for the Is - OCC.gov, https://www.occ.gov/news-issuances/news-releases/2026/nr-occ-2026-9a.pdf 68. Cross Border Payments - PayCompass, https://paycompass.com/blog/cross-border-payments/ 69. Nuclear Power Plant Project Highlights Turkish Role in Russia's Sanctions Evasion - FDD, https://www.fdd.org/analysis/policy_briefs/2025/02/10/nuclear-power-plant-project-highlights-turkish-role-in-russias-sanctions-evasion/ 70. Congressional Testimony - House Committee on Financial Services, https://financialservices.house.gov/uploadedfiles/hhrg-114-ba09-wstate-mmadon-20150616.pdf 71. Chip Poncy - K2 Integrity, https://www.k2integrity.com/en/people/professionals/poncy-chip/ 72. Due Diligence & Risk Assessments - Ankura.com, https://ankura.com/services/due-diligence 73. Juan C. Zarate - FDD, https://www.fdd.org/team/juan-zarate/ 74. Adam Frey - K2 Integrity, https://www.k2integrity.com/en/people/professionals/frey-adam/ 75. FinCEN Proposes New Regulation To Enhance Transparency In Convertible Virtual Currency Mixing And Combat Terrorist Financing - K2 Integrity,

https://www.k2integrity.com/en/knowledge/policy-alerts/fincen-proposes-new-regulation-to-enhance-transparency-in-convertible-virtual-currency-mixing-and-combat-terrorist-financing/ 76. Consilient Announces $3 Million Seed Funding Round for the Development of Next-Generation Financial Crime Compliance Technology, https://consilient.com/consilient-announces-3-million-seed-funding-round-for-the-development-of-next-generation-financial-crime-compliance-technology 77. reaching for a new approach: a newcomer ngo builds a network to fight the modern slave trade, 2012–2018 - Innovations for Successful Societies - Princeton University, https://successfulsocieties.princeton.edu/document/3046 78. 7 AI-Powered RegTech Newcomers to Watch in 2025 - A-Team Insight, https://a-teaminsight.com/blog/7-ai-powered-regtech-newcomers-to-watch-in-2025/ 79. FedScoop: Missing E-Tran controls saw SBA issue $692M in, https://consilient.com/fedscoop-missing-e-tran-controls-saw-sba-issue-692m-in-duplicate-pandemic-relief-loans 80. Vine and Fig Tree Institute I | New York, NY - Cause IQ, https://www.causeiq.com/organizations/vine-and-fig-tree-institute-i,992090467/ 81. Vine & Fig Tree Institute I Inc - Candid, https://app.candid.org/profile/16453107/vine-fig-tree-institute-i-inc-99-2090467 82. Philos Project - Influence Watch, https://www.influencewatch.org/non-profit/philos-project/ 83. Combat Hate Foundation - Influence Watch, https://www.influencewatch.org/non-profit/combat-hate-foundation/ 84. Vine & Fig Tree Fund Inc - Full Filing - Nonprofit Explorer - ProPublica, https://projects.propublica.org/nonprofits/organizations/992100887/202543219349305629/full 85. VINE & FIG TREE FUND INC (EIN 99-2100887) - Grants, Funding, 990s - Impala Digital, https://impala.digital/public/profiles/99-2100887/overview 86. THE PHILOS PROJECT INC (EIN 47-1182714) - Grants, Funding, https://impala.digital/public/profiles/47-1182714/overview 87. Merona Leadership Foundation - Influence Watch, https://www.influencewatch.org/non-profit/merona-leadership-foundation/ 88. CAM Coalition Partners Spotlight: From Grassroots to Institutional Efforts in Stopping Jew-Hatred | Combat Antisemitism Movement, https://combatantisemitism.org/studies-reports/cam-coalition-partners-spotlight-from-grassroots-to-institutional-efforts-in-stopping-jew-hatred/ 89. American Universities Urged to Ensure Safe Campus Environments for Jewish Students During 'Israeli Apartheid Week' | Combat Antisemitism Movement, https://combatantisemitism.org/on-campus/jewish-and-non-jewish-groups-call-on-us-universities-to-ensure-safe-campus-environments-for-jewish-students-during-israeli-apartheid-week/ 90. NEWSLETTER OCTOBER 17TH, 2019 | Combat Antisemitism Movement, https://combatantisemitism.org/newsletters/newsletter-october-17th-2019/ 91. Fake AI 'Rabbis' Push Antisemitic Conspiracies to Millions Online, https://combatantisemitism.org/studies-reports/fake-ai-rabbis-push-antisemitic-conspiracies-to-millions-online/ 92. New CAM Study Exposes Network of Fake AI-Generated 'Rabbi' Accounts Disseminating Antisemitic Tropes on YouTube, https://combatantisemitism.org/studies-reports/new-cam-study-exposes-network-of-fake-ai-generated-rabbi-accounts-disseminating-antisemitic-tropes-on-youtube/ 93. Fake AI 'Rabbis' Spread Antisemitic Tropes in Coordinated TikTok Campaign, New CAM Study Reveals, https://combatantisemitism.org/studies-reports/fake-ai-rabbis-spread-antisemitic-tropes-in-coordinated-tiktok-campaign-cam-study-reveals/ 94. How AI Is Mass-Producing the Oldest Antisemitic Lie, https://combatantisemitism.org/studies-reports/how-ai-is-mass-producing-the-oldest-antisemitic-l

ie/