Trust Tech:

The Emergence of a New Technological Sector for Tackling Online Disinformation and Cognitive Manipulation

Ido Baum, Hod Fleishman, Dalit Gafni, Rotem Kadosh Nussbaum, Naomi Krieger Carmy

July 2025

The College of Management Academic Studies

Brandeis Institute

The Louis Brandeis Institute for Society, Economy & Democracy

REMEDY COLAB

Authors:

• **Dr. Ido Baum**
Academic Director, Brandeis Institute, Associate Professor (Senior Lecturer),
The Striks Faculty of Law, College of Management.
Contact author for Brandeis: ido.baum@brandeis.org.il

• **Hod Fleishman**
Founding Partner, Remedy CoLab & Research Fellow, Brandeis Institute

• **Dr. Dalit Gafni**
Dean, School of Econoomics, College of management

• **Dr. Rotem Kadosh Nussbaum**
Head of Law & Tech Research, Brandeis Institute & Researcher, Hebrew University

• **Naomi Krieger Carmy**
Founding Partner, Remedy CoLab & Research Fellow, Brandeis Institute
Contact author for Remedy CoLab: naomi@remedycolab.com

Acknowledgements

This report is a product of a research project conducted by the Louis Brandeis Institute for Society, Economy and Democracy at the College of Management (Israel) in collaboration with Remedy CoLab. The research was funded entirely by the Brandeis Institute as part of its Social Media Regulation Project. The Brandeis Institute Social Media Regulation project is supported, among others, by the Foundation for Israeli Democracy.

Executive Summary

This report presents the first rigorous research documenting and analyzing the emerging sector of "Trust Tech" – a technological sector aimed at combating online disinformation and digital manipulation.

Findings

- Based on a study of 256 Trust Tech startups around the world, we find that the sector is predominantly based in Western democracies and leading innovation ecosystems, with 46.2% of Trust Tech companies located in the United States, followed by the UK (10.8%) and Israel (4.5%).
- The development of the sector is closely related to global and political events associated with disinformation concerns such as the U.S. elections in 2016 and 2020 and the COVID crisis, with rapidly accelerated growth since 2021. The compounded annual growth rate (CAGR) of number of companies is 18.8% for the 2010-2024 period.
- Funding in the Trust Tech sector is robust but early-stage, with a majority of companies (62.3%) in the Seed funding phase, and averaging $11.6 million raised per company.
- There are already significant success stories, including over 20 companies which have raised over $25M in funding each, and nearly $2 billion in aggregate capital raised, including from global top investors.
- Trust Tech primarily comprises early-stage startups; 86.8% of companies have fewer than 50 employees.
- Trust Tech companies focus on disinformation detection (69.8%) and protection (83.1%), with fewer dedicated to literacy (29.8%) and active mitigation responses (19.2%). Most companies cover multiple areas, reflecting a young field which still lacks deep specialization.
- Relatively few companies offer active mitigation and response solutions, which often rely on Gen AI and other advanced technologies, yet they exhibit the lowest closure rates. This may be the most attractive and promising future development trend.

Recommendations

- Recognizing Trust Tech as a distinct technological sector is critical for market maturation. Recognition of Trust Tech as a distinct sector is essential for enhancing credibility, market access, and investment.
- The rapid growth and robustness of the sector, and the evolution of advanced solutions within it indicate a promising opportunity for innovators and investors.
- As the industry matures and becomes better understood, we expect to see further specialization among companies in terms of solution area and customer profile (public sector, corporate, societal).
- Explicit regulatory frameworks tailored to the unique challenges posed by disinformation are required to standardize practices, establish accountability, and promote industry stability.
- Strategic governmental and institutional support through funding, incentives, and structured market pathways will accelerate innovation, drive economic development, and bolster societal resilience against digital manipulation.

I. Introduction

The digital revolution and advancements in artificial intelligence (AI) have created immense economic, social, and technological opportunities, yet they have also introduced unprecedented challenges. Prominent among these challenges is the issue of digital manipulation, specifically disinformation, defined as intentionally false information disseminated to deceive and influence public perception, attitudes, emotions, and behaviors. This phenomenon is a core element of digital cognitive engineering, which involves deliberate manipulative interventions employing psychological, social, and technological mechanisms, such as narrative distortion, selective or misleading information, and targeting-algorithms. While efforts to influence public opinion have always played a role in political, social, and economic efforts, the digital era has exponentially amplified their scope, speed, and impact. This transformation is driven by the pervasive reach and personalization capabilities of social media platforms—such as Facebook, Instagram, TikTok, X (formerly Twitter), and YouTube—which serve as central vectors for the rapid dissemination of manipulated content. The perfect storm arises from three interconnected forces: the vast data collection and behavioral tracking enabled by social networks, the unprecedented ability of AI to generate persuasive content and convincingly impersonate humans, and the integration of real-world data from mobile devices that describe users' offline behaviors. Together, these forces create a highly targeted, scalable, and personalized manipulation infrastructure that surpasses anything seen in pre-digital eras.

Digital manipulation through social media involves various tactics including large-scale state-sponsored campaigns, astroturfing (creating a false impression of widespread grassroots support), fake news production, deepfakes (highly realistic fake audiovisual content created with artificial intelligence), and social engineering (psychological manipulation to deceive individuals into divulging personal information or adopting specific beliefs).

The harmful impacts of disinformation and digital manipulation span social, political, and economic dimensions. Socially and politically, disinformation erodes public trust in key institutions, exacerbates political and social polarization, and disrupts effective governance.

When public trust diminishes, political divisions deepen, significantly reducing the likelihood of achieving social consensus and effective governance. The destructive influence of disinformation is particularly pronounced during election cycles, where deceptive campaigns aim to manipulate voter attitudes, suppress or inflate voter turnout, and undermine the legitimacy of democratic processes. Beyond elections, misinformation campaigns can incite civil unrest, violent protests, and spread hatred among diverse ethnic, religious, or political groups, even in routine societal contexts. Executing and managing such campaigns requires significant financial and human resources, along with long-term investment.

In the business world, disinformation can destabilize financial markets, damage corporate or individual reputations, and erode public confidence in critical institutions such as health systems - examples of which have been observed during vaccination campaigns, environmental crises, and corporate scandals. This creates a cloud of confusion, impairing rational decision-making at both individual and national levels. Targeted disinformation campaigns aimed at defrauding businesses through social engineering tactics, including attempts to introduce malware via deceptive social media messages or fraudulent links targeting IT departments, or use of deepfakes to circumvent security measures are examples of disinformation spilling over from a national security concern to the business world. False information about companies or stocks can artificially inflate or deflate values, undermining investor confidence and triggering detrimental financial reactions. Additionally, brands face intentional reputational harm through the spread of rumors, orchestrated campaigns, and coordinated negative reviews (review bombing) across digital platforms. Individuals have become targets as well – with high-quality impersonation using deepfakes, campaigns targeting individuals, and AI-driven sextortion.

Addressing disinformation and digital manipulation is therefore an urgent necessity requiring comprehensive responses, regulatory, educational, social, and technological. This has already been recognized on a global scale – most notably by the World Economic Forum which has ranked disinformation as the top short-term global risk to the economy for the past two years in its annual Global Risk Report. Effective strategies must include clear distinctions between legitimate influence (protecting free speech) and harmful manipulation, alongside the development and deployment of advanced technological tools for detecting, monitoring, responding and neutralizing disinformation in real-time.

Companies and innovators have been active in developing and implementing a range of solutions to address these challenges, for governments, businesses, individuals and not-for-profits.

This report outlines the findings of a first of its kind analysis of the emerging sector of technology-based solutions to the multiple harms created by online disinformation and cognitive manipulation. As this sector focuses on defending human trust in the integrity of digital information and consequently on human trust in fundamental political, social and economic institutions and even in other people, we term this emerging technology sector "Trust Tech". While some overlaps with existing sectors (e.g. cyber, risk management, marketing) exist, this is recognized as a unique sector due to specific characteristics, specialized expertise and solutions.

II. The Ecosystem of Solutions

Effectively addressing disinformation and digital manipulation demands a robust, multi-dimensional ecosystem of solutions integrating technological innovation with a viable business model, psychological and behavioral insights, educational / civic initiatives as well as a supportive regulatory climate that can serve as a growth driver for this new domain. This ecosystem aims to detect, counteract, and mitigate manipulative and harmful online content and behaviors, thereby protecting the integrity of digital information environments.

Focusing on technology-based solutions, they can broadly be grouped into nine categories, that span four broader categories: Providing end users with **information literacy and consumer tools**, assisting in the **detection** of disinformation, helping **protect** against disinformation and providing active **mitigation and response:**

Broad Category	Detailed Category	Definition	Example Keywords
LITERACY	Information Literacy & Consumer Tools	Digital tools aimed at empowering individuals through digital literacy, awareness and skills training; or consumer tools enabling individuals to gain transparency, verification or protection from harmful content..	Media literacy, fact-checking plugins, critical consumption tools, source rating, bias flags, user education, verification aids, misinformation game, new social media platform
DETECT	Disinformation Detection	Technologies that detect and flag manipulated, false, or misleading content across formats (text, video, image, audio). Some tools and solutions in this category come from the field of Open Source Intelligence (OSINT).	Deepfake, fake news, detection AI, misinformation scanner, video forensics, linguistic deception, NLP classifiers, fake tweet detection, audio authenticity, forensic watermarking, sentiment analysis
	Authentication & Provenance	Technologies that verify content origin and ensure its integrity throughout the content lifecycle, sometimes via technologies such as blockchain.	Media provenance, cryptographic hashing, watermarking, blockchain traceability, authenticity certificate, digital fingerprinting, tamper detection, content signature
	Identifying context, narratives and actors	Solutions that trace the evolution of disinformation narratives and/or map the influence of agents or networks behind them, including identifying inauthentic online actors (bots, sock puppets), and behaviors	Narrative tracking, narrative intelligence, actor mapping, bot detection, troll farms, hashtag analysis, meme evolution, coordination detection, influence modeling, sockpuppet networks, covert campaign

PROTECT	Content Moderation & Safety	Solutions or tools that remove, flag, or limit access to harmful or deceptive content using rule-based or AI filters.	Toxicity filtering, hate speech detection, policy enforcement, takedown engine, safety layer, Trust & Safety API, automated moderation, policy violation flags,
	Identity & Fraud Prevention	Systems that protect platforms from bots, fake accounts, and impersonation, often with biometric or behavioral authentication.	Fake account detection, liveness detection, bot filtering, behavioral biometrics, impersonation shield, identity graph, fraud scoring, sybil resistance; social engineering, KYC, KYB, AML, anti money laundering, phishing, spear fishing, code attacks, attack surface analysis, cyber risk, social engineering
	Reputation & Privacy Protection	Solutions designed to protect individuals and organizations from reputational damage or privacy violations caused by disinformation, doxxing, or digital impersonation.	reputation monitoring, defamation response, doxxing protection, impersonation takedown, digital rights defense, personal data leak alert, reputation repair, digital identity cleansing, brand protection
	LLM Safety	Tools and frameworks that ensure the safe and responsible use of large language models, especially in avoiding model misuse for generating or amplifying disinformation.	LLM safety, prompt injection defense, hallucination filter, misinformation prevention, AI output moderation, adversarial prompting detection, generative AI safeguards, model misuse detection
RESPOND	Active Mitigation and Response	Platforms and services that use advanced mitigation strategies – e.g. craft, deploy, or test counter-narratives to disinformation — aiming to reduce its influence through persuasive or corrective communication.	counter narratives, digital inoculation, persuasive debunking, narrative correction, strategic comms, pro-social messaging, refutation design, audience-tailored rebuttal, mitigate attacks, disrupt attacks, counter messaging, active response, mitigation, takedown, account blocking.

Despite considerable technological advancements, currently, human expertise remains indispensable within this ecosystem. Skilled analysts play a pivotal role by contextualizing data within broader political, social, and cultural frameworks, ensuring accurate threat assessment and response effectiveness. However, reliance on a "human in the loop" also slows down the detection and response cycle, increases the cost of defending against disinformation and therefore limits its effectiveness. Recent development in the field of generative AI could help mitigate these inefficiencies.

It is important to note that technological solutions could be developed as features from within existing large tech players (social media platforms), by new companies (start-ups) or by not-for-profit players. We focus on standalone company solutions in this report.

This emerging ecosystem of solutions has overlap with other industry verticals – most notably cyber security, but also trust & safety, digital marketing, authentication, reputation and risk management, and even ed-tech. Trust Tech is a distinct emerging industry with its own aims, solutions, expertise and focus areas. Limited academic and industry efforts to date have attempted to define the sector or variants of it with names such as “anti-disinformation tech”, “cyber influence”, “narrative defense”, “narrative intelligence” and “trust ops”. This is the first broad mapping and analysis of this scale, and we define the field as Trust Tech.

III. The Trust Tech Database: Data Collection Methodology

This research utilized a rigorous and comprehensive methodology to construct an exhaustive database of companies operating within the Trust Tech sector, leveraging Crunchbase as the primary data source. Crunchbase is recognized globally as a reliable repository containing extensive quantitative and qualitative information on innovative companies, startups, investments, and market dynamics.

Initially, we identified Trust Tech companies through targeted keyword searches within Crunchbase, employing terms specifically related to disinformation, digital manipulation, cognitive engineering, misinformation, narrative detection, bot mitigation and other related terms. This initial screening process generated a preliminary dataset comprising over 900 companies.

To ensure precision and relevance, we conducted a detailed manual filtering process. Each company's operational nature and relevance to the Trust Tech sector were reviewed. Following this review, the refined dataset included 256 companies explicitly engaged in developing technological solutions against disinformation and digital manipulation, in a broad sense. This means solutions cover a diverse area in terms of the target industries and issues (solutions for national security, brand protection, societal disinformation and more) as well as in terms of the nature of the solution (detection tools, authentication tools, social media platforms built to protect from disinformation and more).
To further enhance the robustness of our dataset, we supplemented the Crunchbase information by manually collecting additional detailed data from the official websites of these 256 companies, where available. This approach allowed us to capture additional data not initially provided to Crunchbase, and to identify 94 of the 256 companies which were no longer active (though still providing valuable insights).
The final comprehensive dataset enabled us to perform a comparative analysis with related technological sectors, also retrieved from Crunchbase, notably a selection of cybersecurity companies (914 companies, several sub-verticals) and influencer marketing (1,994 companies, a sub-section of digital marketing). These comparative evaluations have provided substantial insights into market structure, market trends, patterns of investment and funding.

Some caveats. This study has some methodological limitations that should be considered when interpreting the findings. Data on certain parameters was unavailable for significant numbers of companies, so the analysis for each parameter was conducted based on available data only. Crunchbase, although widely recognized as a reliable data source, contains some information that relies on self-reported details from companies.

Despite these limitations, the dataset remains sufficiently robust and reliable for identifying overall trends and comparative patterns within the market, especially concerning mature and established companies.

IV. The Trust Tech Sector: The Numbers

This chapter presents descriptive statistics on the 256 companies included in our Trust Tech sector database. We examine key indicators—including company establishment timelines, geographic distribution, revenue levels, funding statuses, employee numbers, and market visibility.
To better understand the descriptive data of the Trust Tech industry, we chose a sub-selection of two established sectors as comparative benchmark industries: cyber security and digital marketing, each one with key similarities to Trust Tech.

Digital marketing is a vast sector of over 77,000 companies – we selected the sub-sector of influencer marketing (1,994 companies). Cyber security is also a huge sector with over 33,000 companies – we chose three sub-verticals: mobile security, zero trust and IOT security (altogether 914 companies).
By evaluating key performance metrics, including year of establishment, geographic distribution, funding profiles, employment sizes, public visibility, founder structures, investment patterns, and market longevity, this analysis provides essential insights into the relative maturity, operational characteristics, and growth dynamics of the Trust Tech sector.

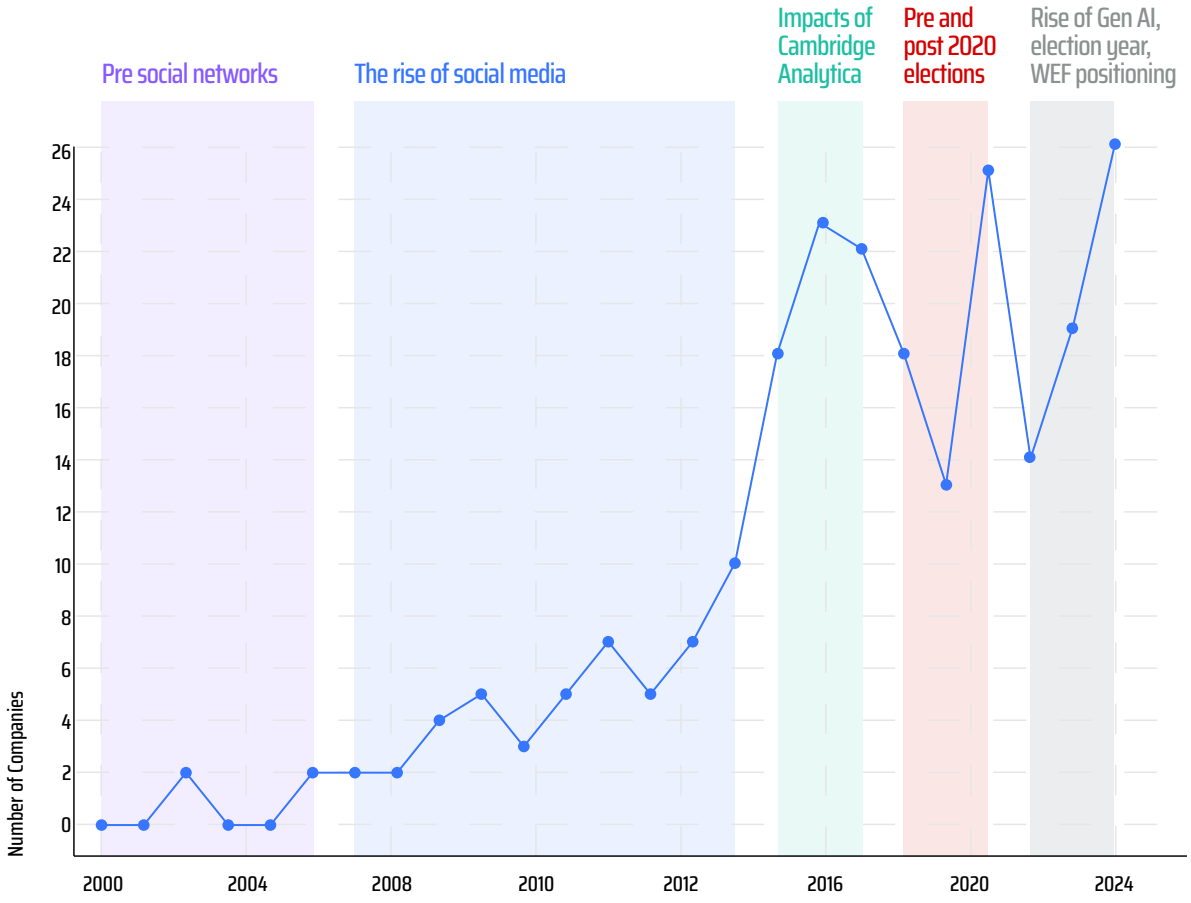
1. Year of Establishment:

Data was available for approximately 91% of the total sample. The data reveals the sector's nascent nature, with approximately 92% of Trust Tech companies founded after 2010, reflecting the increased importance and widespread adoption of social media platforms. A notable acceleration is observable since 2016 and especially between 2021 and 2024, peaking in 2024 with 26 companies established.
This surge aligns closely with significant global events and disruptions, such as the 2016, 2020, and 2024 U.S. elections, and the COVID-19 pandemic, which heightened awareness and urgency surrounding digital manipulation issues. Recognition of the issue, notably by the World Economic Forum in 2023,
also drove interest. Concurrently, advances in Generative AI (GenAI) and the growing importance of Large Language Models provided both challenges and innovative solutions, driving demand for Trust Tech products and services.

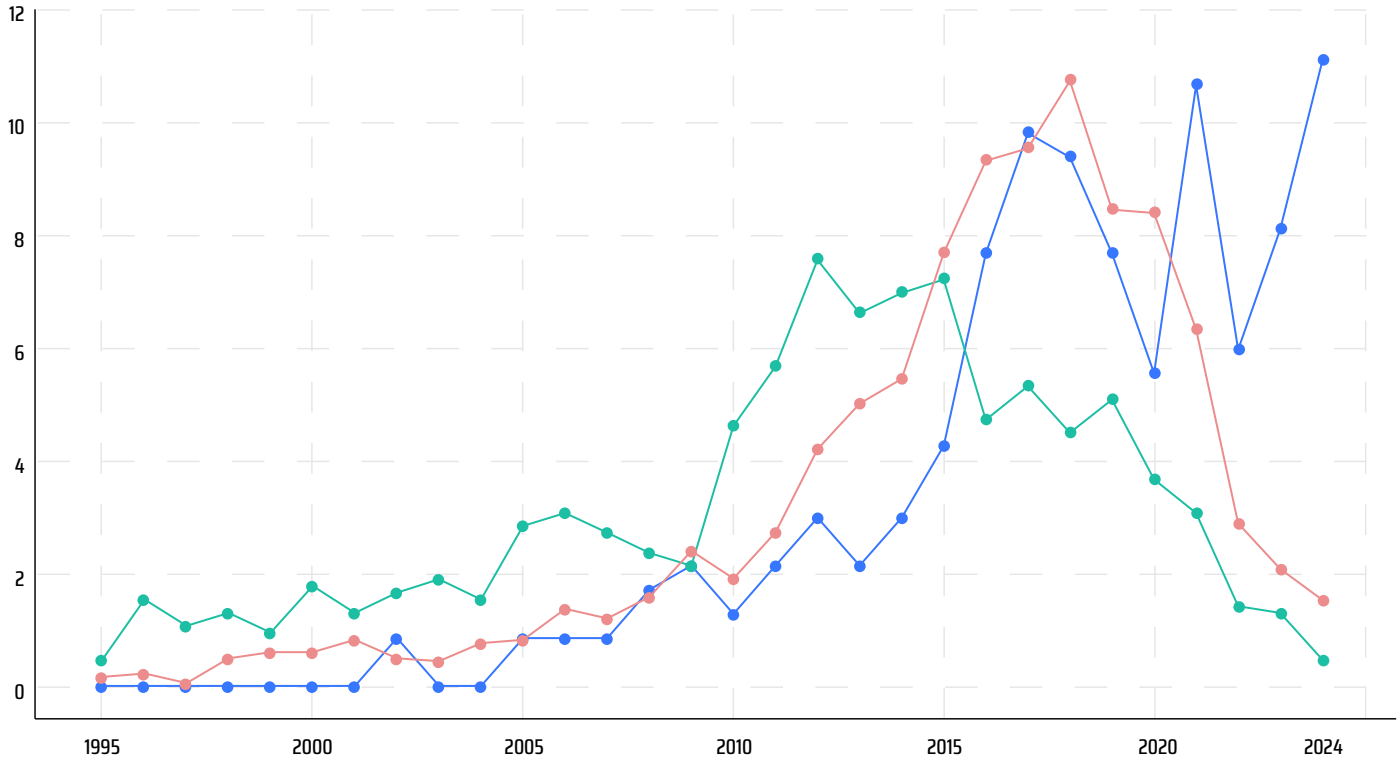
When compared to benchmark sectors, Trust Tech exhibits notably distinct growth patterns. Over 81% of Trust Tech companies were established after 2015, indicating a rapid, recent expansion driven by global socio-political events and technological developments. In contrast, influencer marketing shows steadier, incremental growth across a more extended timeline, reflecting a more mature market development. Cybersecurity, the most mature sector of the three, has approximately 70% of its companies founded prior to 2016, signaling industry consolidation and stability.

Looking at the average growth rate of the sectors in terms of number of companies, Trust Tech has a CAGR of 18.8% in the period 2010-2024 (the main period since the sector came into existence), compared to a CAGR of 15.8% and 13.5% for marketing and cyber benchmarks respectively during a comparable 14-year period in the industries' early days, 1995-2009.

Trust Tech: Number of companies founded in each year



Growth Trend in Companies Founded per Year



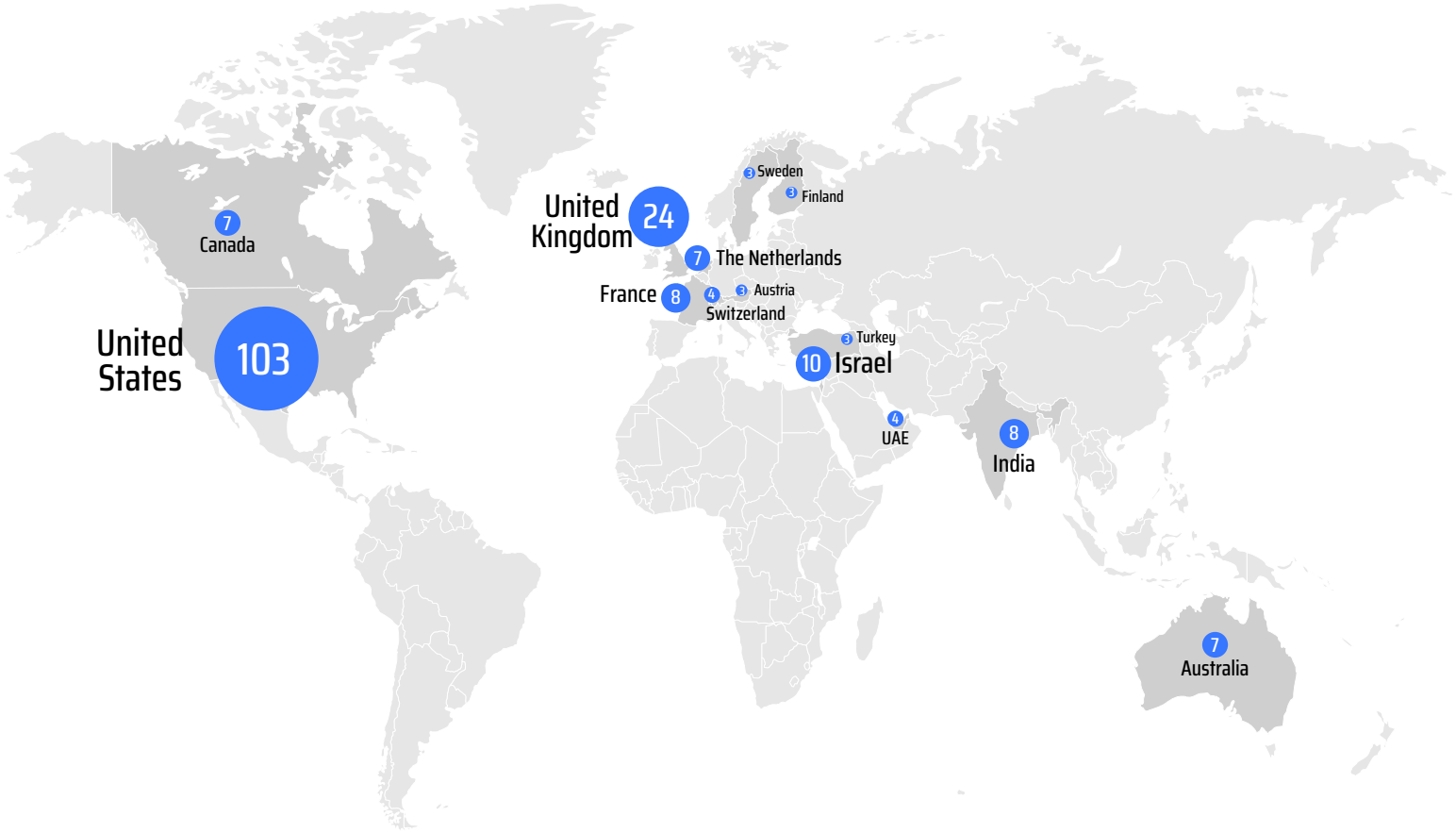
Trust Tech (scaled 1: 2.3)
Cyber benchmark (scaled 1:8.5)
Digital Marketing benchmark (scaled 1:18.3)

2. Geographic Distribution

Location data was available for 87% of the Trust Tech companies analyzed, indicating a clear geographical concentration within globally recognized innovation ecosystems, predominantly in Western democracies. The United States emerges prominently, hosting 46.2% of Trust Tech companies. Following the U.S. are the United Kingdom (10.8%), Israel (4.5%), and France, India, and the Netherlands (each at 3.6%). These rankings are similar to global startup ecosystem rankings, but with some key variances. Notably, some significant global innovation hubs in non-democratic countries or limited democracies like Singapore and China, ranked fifth and thirteenth respectively in overall start-up ecosystems, lack representation in the Trust Tech sector. Conversely, India, despite its lower global ecosystem rank (nineteenth), has a vibrant community actively addressing fake news and trust issues, placing it fifth in terms of Trust Tech presence. Overall, more than 70% of Trust Tech companies are concentrated within just eight countries, reflecting the critical influence of available tech talent and expertise in related fields such as cybersecurity, intelligence, and digital marketing.

Unsurprisingly, the United States also significantly dominates the benchmark sectors examined in the study: influencer marketing (34%) and cybersecurity (47.7%). Influencer marketing, however, demonstrates broader global dispersion with strong presence in emerging markets, notably India (15.7%). Cybersecurity firms exhibit notable concentrations within advanced technological and security-focused countries, including a significant cluster in Israel (3.9%), reflecting strategic and national security priorities. Trust Tech's pronounced presence in democratic nations underscores the inherent relationship between democratic governance structures and proactive measures against disinformation and digital manipulation.

Top 10 Global Locations – Headquarters of Trust Tech Companies

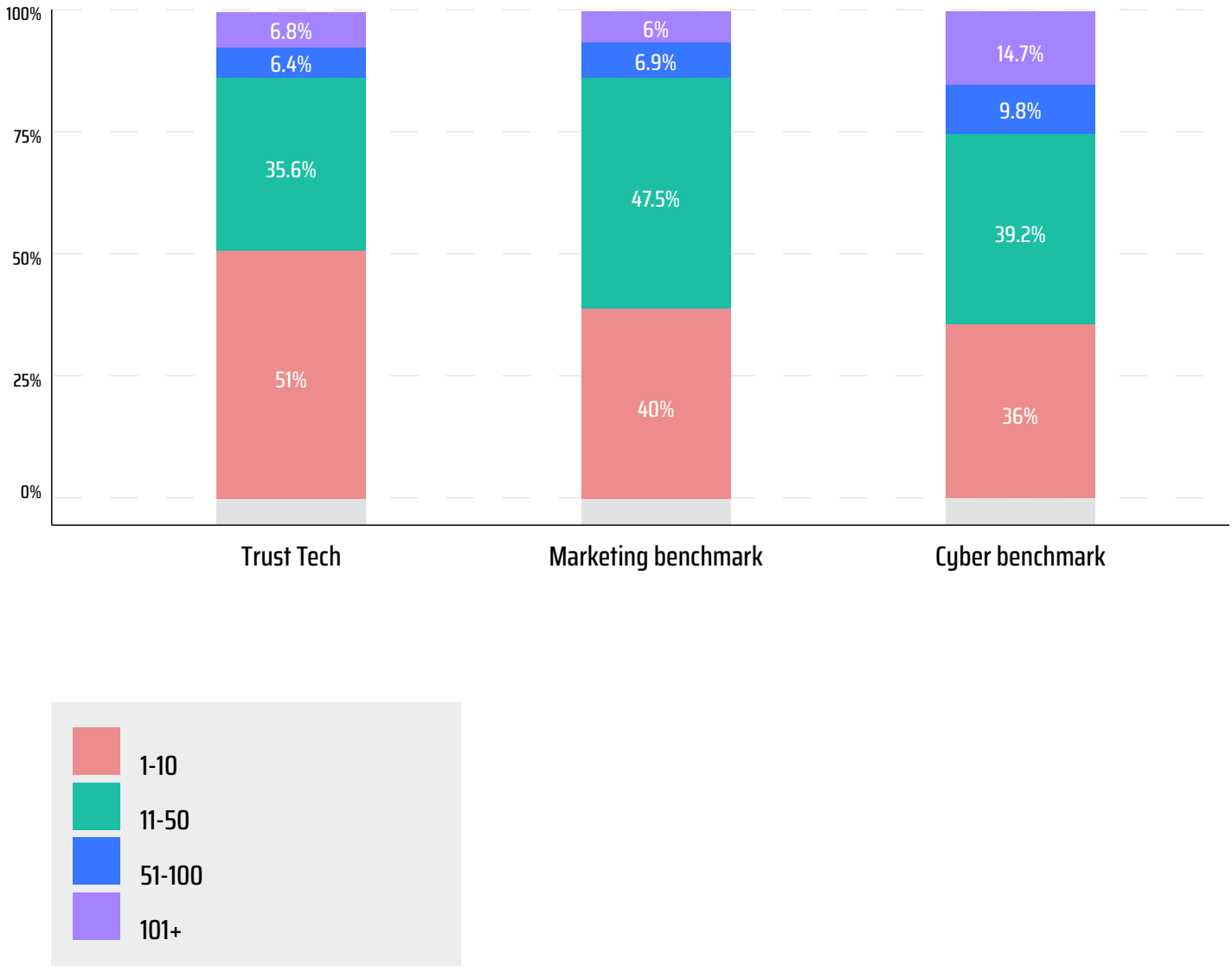


3. Number of Employees:

Employee data, available for 92% of Trust Tech companies, reveals the sector's characteristic early-stage profile. Approximately 51.2% of companies maintain small teams consisting of 1–10 employees, and 35.6% employ between 11–50 individuals. Only a limited number of companies (13.1%) have surpassed the 50-employee mark. The team sizes reflect the early stages of the sector, and may indicate a pre-scale phase where companies are taking their first steps in the market but have not yet gained significant momentum.

By contrast, influencer marketing companies typically maintain slightly larger workforce sizes, indicative of their more mature operational frameworks and established market presence. Cybersecurity firms stand apart with approximately 15% employing over 100 employees, reflecting significant market maturity, complex organizational structures, and established operational capacities.

Number of Employees – Trust Tech companies vs. Benchmark sectors



4. Public Visibility (Articles)

Public visibility, gauged through the average number of articles mentioning each company, serves as an indicator of market interest and relevance. Visibility data was available for 56% of the Trust Tech companies, revealing an average of 18.9 mentions per company. This level of visibility suggests considerable engagement and interest from media, academia, and governmental entities, reflecting both the societal impact and strategic importance of the sector. While heightened visibility offers opportunities for growth and legitimacy, it simultaneously carries risks of increased scrutiny and regulatory challenges. Comparatively, cybersecurity firms exhibit the highest level of public visibility, averaging approximately 36 mentions per company, indicative of the sector's critical role in national security and robust public interest, as well as the higher business profile of companies raising funding and closing deals. Influencer marketing, despite its substantial market presence, registers lower visibility, averaging about 12 mentions per company. This lower visibility aligns with its primarily commercial and often "behind the scenes" orientation, attracting less intensive scrutiny compared to sectors engaged with broader societal and political implications.

5. Number of Founders:

Founder data, available for 71% of Trust Tech companies, reveals a typical early-stage startup structure, averaging 1.84 founders per company. This is typical of entrepreneurial ventures led by small, collaborative teams.

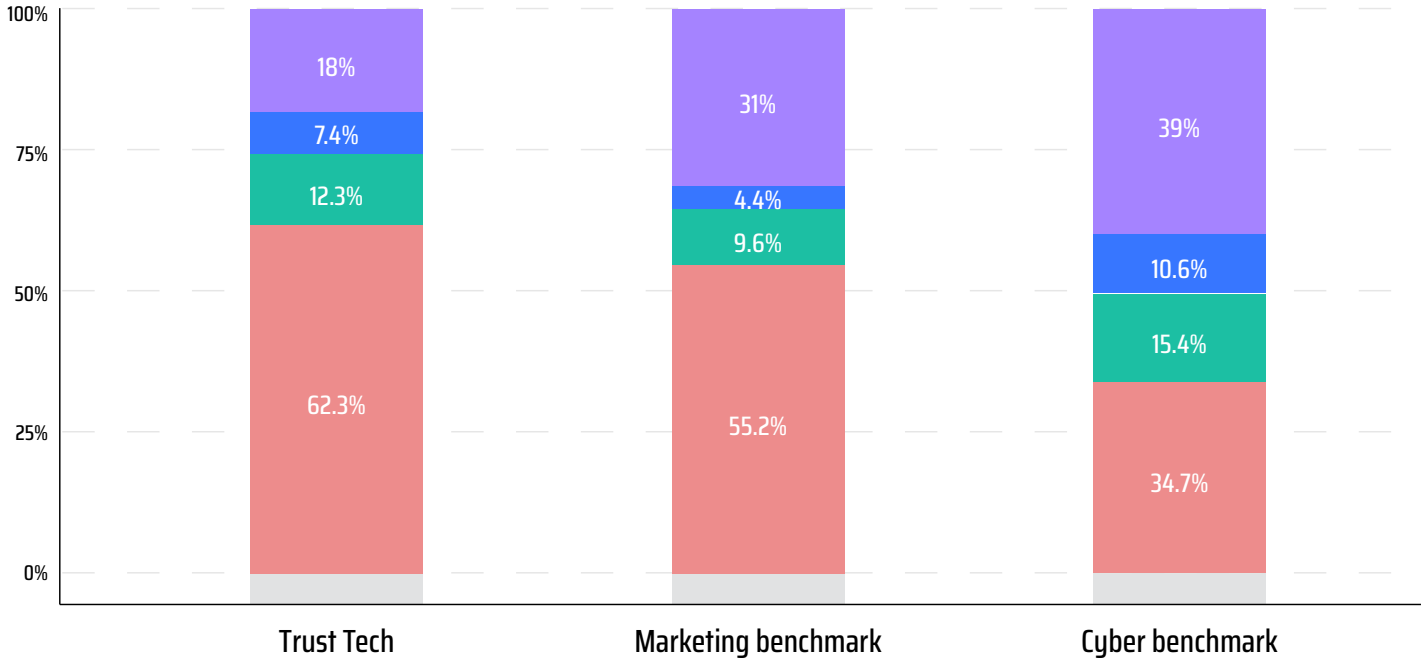
This is similar to the cybersecurity average of 1.81 founders per company, highlighting an analogous collaborative entrepreneurial approach indicative of industries emphasizing technological innovation and strategic development. In contrast, influencer marketing firms often feature single-founder structures – 1.56 founders on average and 62% of companies with a sole founder, reflecting independent and commercially mature operational models.

6. Funding Status

Funding status data was available for approximately 48% of Trust Tech companies. Analysis reveals a clear predominance of early-stage investment, with 62.3% of these companies currently at the Seed funding stage, 23.8% at Pre-Seed/Angel stage, and 12.3% at the Early Stage Venture level. Notably, only a small proportion (7.4%) have progressed to advanced stages such as Late Stage Venture, IPO, or Private Equity. Additionally, 18.3% of companies reported undergoing mergers and acquisitions (M&A), indicating an active consolidation process within the industry, though lower than the benchmark industries.

In comparison, influencer marketing firms exhibit a distinctly different funding profile, with 55% at Seed funding stage, and 30.9% M&A. This is indicative of a more mature market, which may also be self-sustaining driven by established revenue streams, and less venture funding. Cybersecurity companies show a more balanced funding distribution, with 34.7% seed funding and 10.6% late stage, IPO of Private Equity. This reflects industry maturity and persistent investor interest, with more market stability relative to the nascent Trust Tech sector.

Funding Status – Trust Tech companies vs. Benchmark sectors

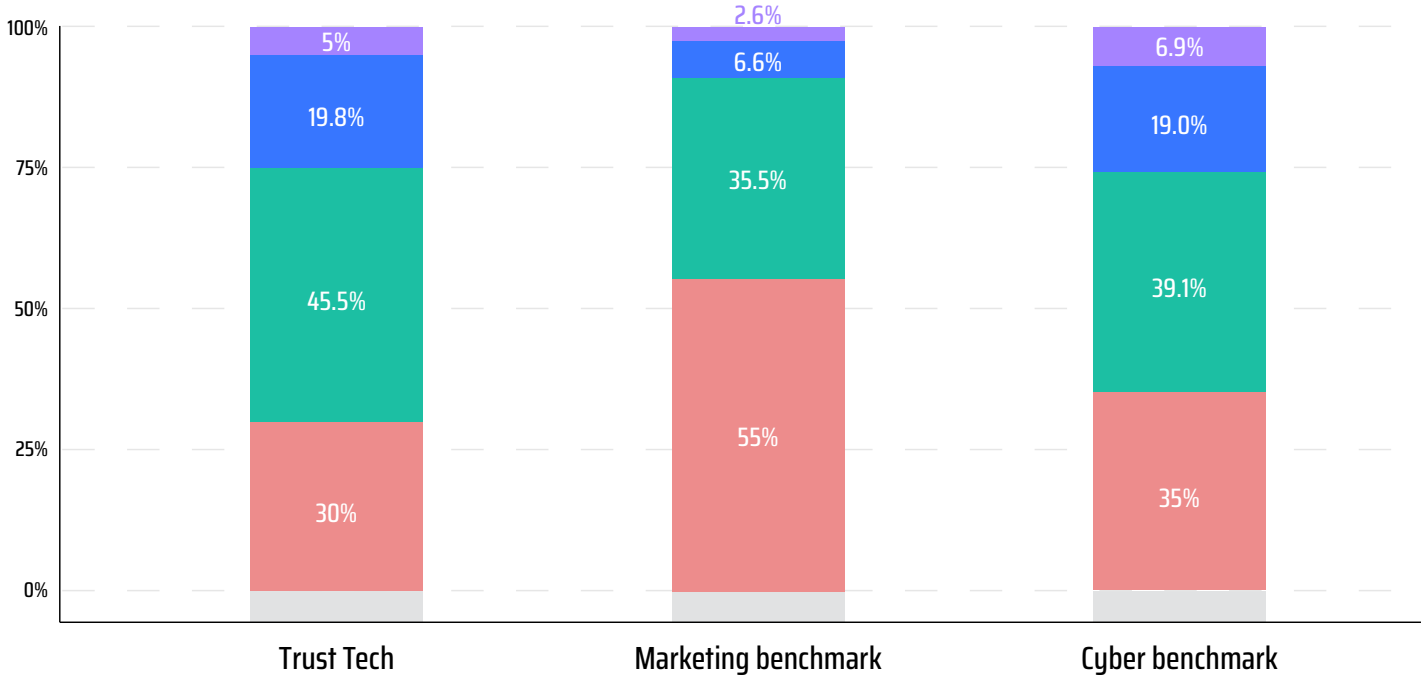


7. Funding Rounds and Amounts:

Funding round data was available for 54% of Trust Tech companies, revealing an average of approximately 2.2 funding rounds per company among those that raised funds. Total funding amounts, reported by 39% of companies, averaged around $11.6 million per company. Equity funding, specifically reported by 38% of the firms, averaged approximately $11.0 million, closely aligning with total funding figures and reinforcing the prevalence of equity financing typical for early-stage technology ventures.

In comparative terms, Trust Tech companies attract substantial investor interest, reflected by their relatively robust average funding rounds and amounts. Cybersecurity firms, however, demonstrate higher average funding levels, approximately $18.4 million per company, due to mature investment ecosystems and the strategic importance of cybersecurity solutions. Influencer marketing entities generally report lower funding amounts, averaging about $6.8 million, which may align with more revenue-driven and independently sustainable business models, necessitating fewer external investments.

Total Funding Raised ($ USD) – Trust Tech vs. Benchmark Sectors



8. Investor Profiles:

Lead investor data, available for 32% of Trust Tech companies, reveals an average of 2.17 lead investors per company, indicating a distribution of investment risk common in nascent industries. On average, Trust Tech companies have about 5.8 total investors each, highlighting a reliance on a relatively diverse investor base typical of early-stage ventures seeking cautious yet supportive investment strategies.

The Trust Tech profile is similar to cybersecurity in this regard, which has an average of 2.2 lead investors and 4.8 total investors. Influencer marketing, in contrast, has lower averages of 1.6 lead investors and 3.6 total investors, probably reflecting a more self-sustaining business model.

9. Time to Exit:

Data regarding closures (companies that discontinued operations) and exits (companies that went public on the stock exchange or were sold to another company) in the dataset were limited. While it is difficult to assess average time to closure, the data indicates an exit rate of approximately 9% with an average exit time of 6.1 years. These metrics are characteristic of early-stage, high-risk technology sectors, yet may indicate a higher than normal exit rate particularly in terms of time to exit. The global standard is normally about 10 years to exit.

Average exit times in Trust Tech are shorter compared to influencer marketing (7.7 years, 6% of companies) and notably cybersecurity (approximately nine years, 18% of companies). This may indicate a still-formative market with limited documented exits, but may also reflect the interest in Trust Tech solutions and the relevance to integrate them into broader offerings via acquisitions by social media platforms, advertising firms and other companies.

Cybersecurity's extended lifespans and higher exit rates reflect market stability and maturity, while influencer marketing's limited exits may suggest sustained independent operations without frequent mergers or public offerings.

Collectively, these statistics present a clear picture of the Trust Tech sector as an early-stage, rapidly emerging market driven by global events and technological innovation. The sector shows significant promise and is comparable to other start-up sectors in key parameters – notably, it aligns more closely with cyber security than with influencer marketing. However, the sector is still relatively small and limited in data.

10. Analysis of companies by substantive areas of activity

Based on analysis of the descriptions of the companies, their products and services as described in Crunchbase and supplementing information from their websites, we divided the field into 9 substantive categories or "tags" which represent the focus areas and offerings. The categories were then grouped into four broader categories which align with the stage of response to disinformation and related harms. This is a framing which is accepted in the field, a prominent example being the DISARM framework which breaks down the structure of narrative attacks into stages.

Broad Categories	% of cos tagged	Detailed Categories	Distribution within the category
1) Literacy	29.8%	Information Literacy & Consumer Tools	
2) Detect	69.8%	Disinformation Detection	59.2%
		Authentication & Provenance	22.0%
		Identifying context, narratives and actors	19.2%
3) Protect	83.1%	Identity & Fraud Prevention	40.8%
		Reputation & Privacy Protection	37.3%
		Content Moderation & Safety	35.3%
		LLM Safety	9.4%
4) Respond	19.2%	Active Mitigation And Response	

Our finding show that most companies have multiple "tags" and belong to several categories – this reflects a key finding regarding the industry: It is still relatively "crowded" with companies attempting to cover most problem areas and not offering narrow specialization. 87% of companies cover at least two of the nine detailed categories, and 79% of companies cover at least two of the broader four categories. However, the overall picture of the industry shows a clear pattern:

a) The "core" of the industry is detection and protection solutions. 70% of companies offer detection solutions and 83% offer protection. The other two categories are the "outskirts" of the industry – on one hand, tools that are aimed more at individuals and offer more basic solutions including a focus on information literacy and building resilience (30% of companies); and at the other end the still relatively rare but potential "holy grail" of active response and mitigation solutions (19% of companies).

b) The rate of active companies (included acquired ones) vs. closed companies varies significantly between categories. In the "Literacy" category, over 54% of companies closed – possibly reflecting more challenging business models and lower technological sophistication. In the core categories of Detect and Protect, 33% of companies have closed. In the "Respond" category only 27% of companies have closed, potentially reflecting both a newer category and higher promise in terms of technology and market application.

Distribution of Companies across Counter-Disinformation Phases

(Each company can be "tagged" in multiple categories – i.e. there is overlap between categories)

V. Conclusions: Why Recognizing the Trust Tech Sector Is Critical

The Trust Tech sector demonstrates clear characteristics of an emerging, innovation-driven market, distinct from the financial maturity and strategic significance of cybersecurity and differing substantially from the revenue-centric, independent operational frameworks of influencer marketing. Trust Tech companies exhibit rapid recent establishment, concentrated geographic clustering within innovation ecosystems and democracies, early-stage revenue structures, robust early-stage investor interest, modest employee numbers, moderate-to-high public visibility, collaborative founder structures, and relatively short operational lifespans thus far.

From a nearly non-existent field before the year 2005 to over 250 companies today (160 active companies), this is a rapidly growing sector. When we look at the compounded annual growth rate (CAGR) in number of companies, we see an average annual rate of 18.8% in recent years, which is significantly higher than the benchmark industries even when looking at comparable periods of their formative growth.

	Trust Tech	Marketing benchmark	Cyber Benchmark
CAGR 1995-2009	N/A	15.8%	13.5%
CAGR 2010-2024	18.8%	14.2%	7.5%
CAGR 2015-2024	17.4%	10.5%	4.0%

Looking at the leading companies in the industry – those who have raised over $25M in funding – shows a promising story: nearly $2 billion in aggregate capital raised by 23 companies; and investment by top global names such as Andreessen Horowitz, SoftBank Vision Fund, M12 - Microsoft's Venture Fund, Y Combinator, Index Ventures and more. Interestingly, when looking at the top companies by funding amounts, 70% (16 out of 23) are US-based, with the next place going to Israel – 13% (3 out of 23). No other country has more than one company on this shortlist.

On the demand side, the drivers of the industry remain strong and becoming stronger, with the rapid pace of GenAI development and adoption, the continued growth of social media and the "influence economy", the widespread adoption of synthetic content (AI-generated text, images and videos), targeting and hyper-personalization abilities – and the use of all these to influence, attack and undermine across sectors. Adding to the demand side is the growing recognition of the harmful impact of online disinformation by governments and organizations such as the World Economic Forum.

At the same time, the industry is still small in number of companies and in their size, and still in early days in terms of investor recognition, clear go to market strategies and revenue growth. Confusion between the national / societal / business use cases of the solutions, relatively early days in terms of real-world impacts that can be reported, and the high cost of scaling solutions hinder a compelling market opportunity story.

These comparative insights indicate Trust Tech's growth trajectory and strategic potential, but also hint to the critical need for sustained investor support, robust regulatory frameworks and/or government incentives to drive a sector with national security and economic implications, and clearer business models and scalable technology solutions to facilitate market maturation.

Addressing the growing challenges of disinformation and digital manipulation, and considering the positive impact of regulation and industry recognition on the growth of comparable industries such as the cyber security sector, necessitates the formal recognition and clear definition of Trust Tech as a distinct technological sector. This recognition is critical for several reasons.

Firstly, formal industry recognition legitimizes Trust Tech, enhancing credibility and fostering confidence among customers, investors, and regulators. Clearly defining the sector positions companies as stable, reliable, and aligned with established standards, significantly improving access to funding sources such as venture capital, governmental grants, and institutional investments. Industry recognition includes certifications that validate technical compliance, awards and rankings like the Cyber Security Awards, strategic partnerships with major tech firms, and endorsements from trusted independent bodies such as the EU Disinfo Lab.

Secondly, without formal recognition, Trust-Tech companies encounter prolonged sales cycles and ambiguity regarding responsibility within client organizations, should this be handled by the CISO? Marketing? Or the Risk Management team? Such hurdles are reminiscent of the early days for other tech sectors. Establishing Trust Tech as a recognized sector enables clearer budget allocations, defined entry points, and specialized organizational roles, thereby facilitating smoother market entry and operations.
Thirdly, explicit regulatory frameworks tailored to the unique challenges of disinformation and digital manipulation are essential. Such clarity ensures standardized practices that effectively mitigate risks, establish accountability, and provide consistent protection against digital threats.

Moreover, defining Trust Tech as an independent sector with technological challenges and promising growth potential attracts talent, drives innovation, and promotes competitive development, contributing significantly to economic growth and job creation. Clearly articulated industry standards and best practices enhance operational efficiency, build public and corporate trust, and strengthen market appeal for the products and services offered.

Ultimately, formally establishing Trust Tech is more than symbolic-it represents a foundational step that fosters market growth, industry stability, ongoing innovation, and broader societal resilience against the increasingly pervasive effects of digital manipulation.

About Brandeis Institute

The Louis Brandeis Institute for Society, Economy and Demicracy, established in Israel in 2022 and hosted at the College of Management (COLMAN)-Israel's first private college-is an international research institute dedicated to fostering a more democratic, equitable, and innovative society. It conducts both theoretical and applied research, spanning the social sciences, economics, finance, law, regulation, media studies, and the exact sciences.

Named for Louis D. Brandeis-renowned U.S. Supreme Court Justice, Zionist leader, and trailblazer in exposing the dangers of economic concentration-the Institute draws inspiration from his belief that concentrated economic power undermines democracy. Its work emphasizes rigorous research driving robust policy recommendations, community-building, organizing conferences, discussions, and publications to engage academics, practitioners, and the public.

Among the Institute's key initiatives is the study of social media's impact on national security, democracy, and education. Its pioneering Big Tech and democracy project focuses on legal, regulatory, and technological strategies to curb disinformation, foreign information manipulation, hate speech, and extremist content on major platforms. This initiative underscores the Institute's commitment to confronting critical challenges facing Israel, Jewish communities worldwide, and democracies at large-offering insights that inform societies globally.

The Brandeis Institute benefits from an international academic advisory board composed of globally recognized scholars and practitioners.The Institute is led by its academic director, Dr. Ido Baum, An Associate Professor (senior lecturer) of Law and Economics at COLMAN's Haim Striks Faculty of Law.

About Remedy CoLab

Remedy CoLab is a boutique advisory firm specializing in strategies and solutions to address content manipulation, digital disinformation, and online influence in the context of social media and artificial intelligence.
Remedy is a domain expert in this field of challenges and in the emerging field of Trust Tech.

The firm applies a multidisciplinary approach that integrates subject-matter expertise, technological insight, and collaboration with a broad network of practitioners. Its work includes designing and implementing countermeasures to malicious online activity, supporting organizational resilience, and advising public, private, and nonprofit actors. Remedy also contributes to ecosystem-building by advising funders and stakeholders on innovation and investment opportunities.

Founded by Naomi Krieger Carmy and Hod Fleishman — professionals with backgrounds in technology, business, and social impact — the company operates globally, with a particular emphasis on leveraging Israeli innovation in response to these global challenges.