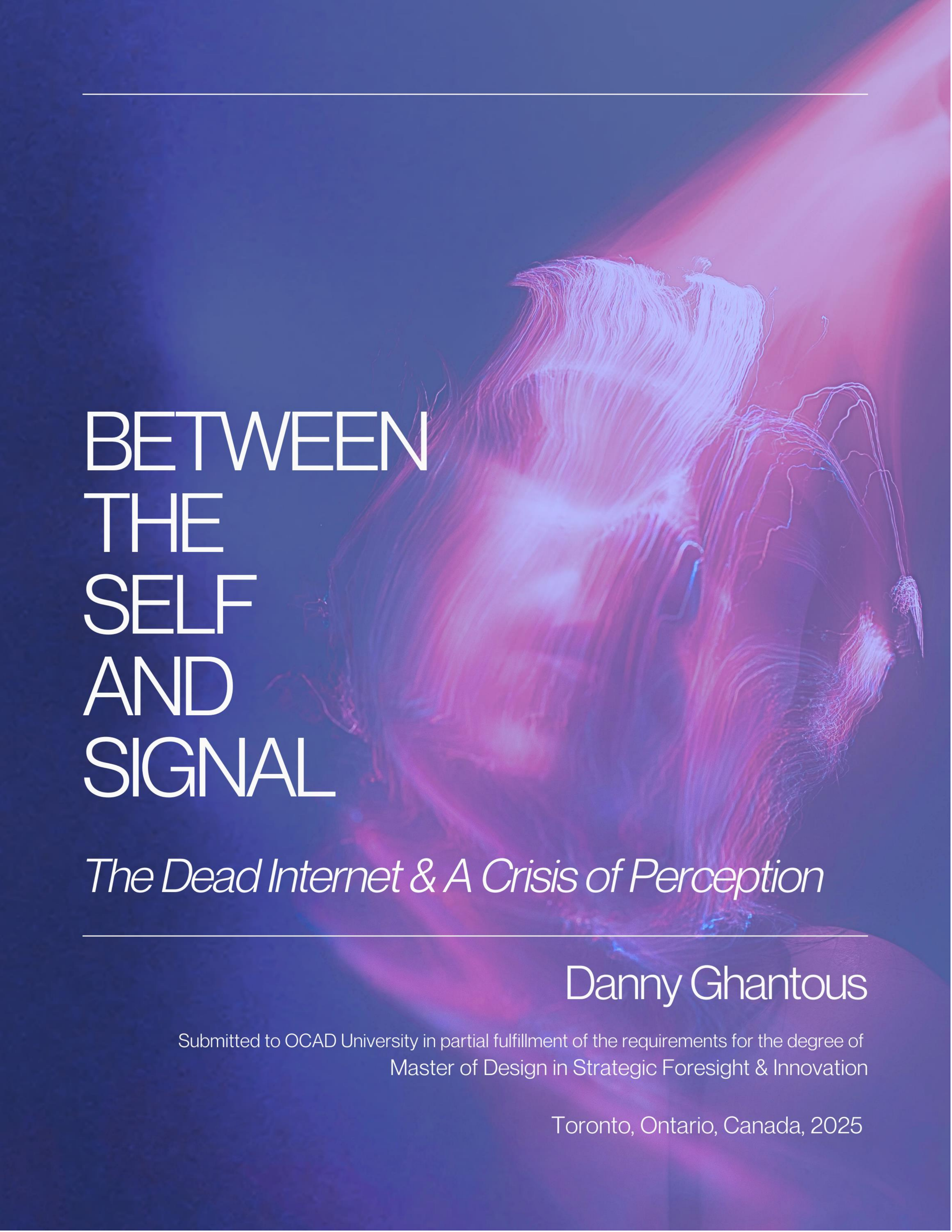


BETWEEN THE SELF AND SIGNAL

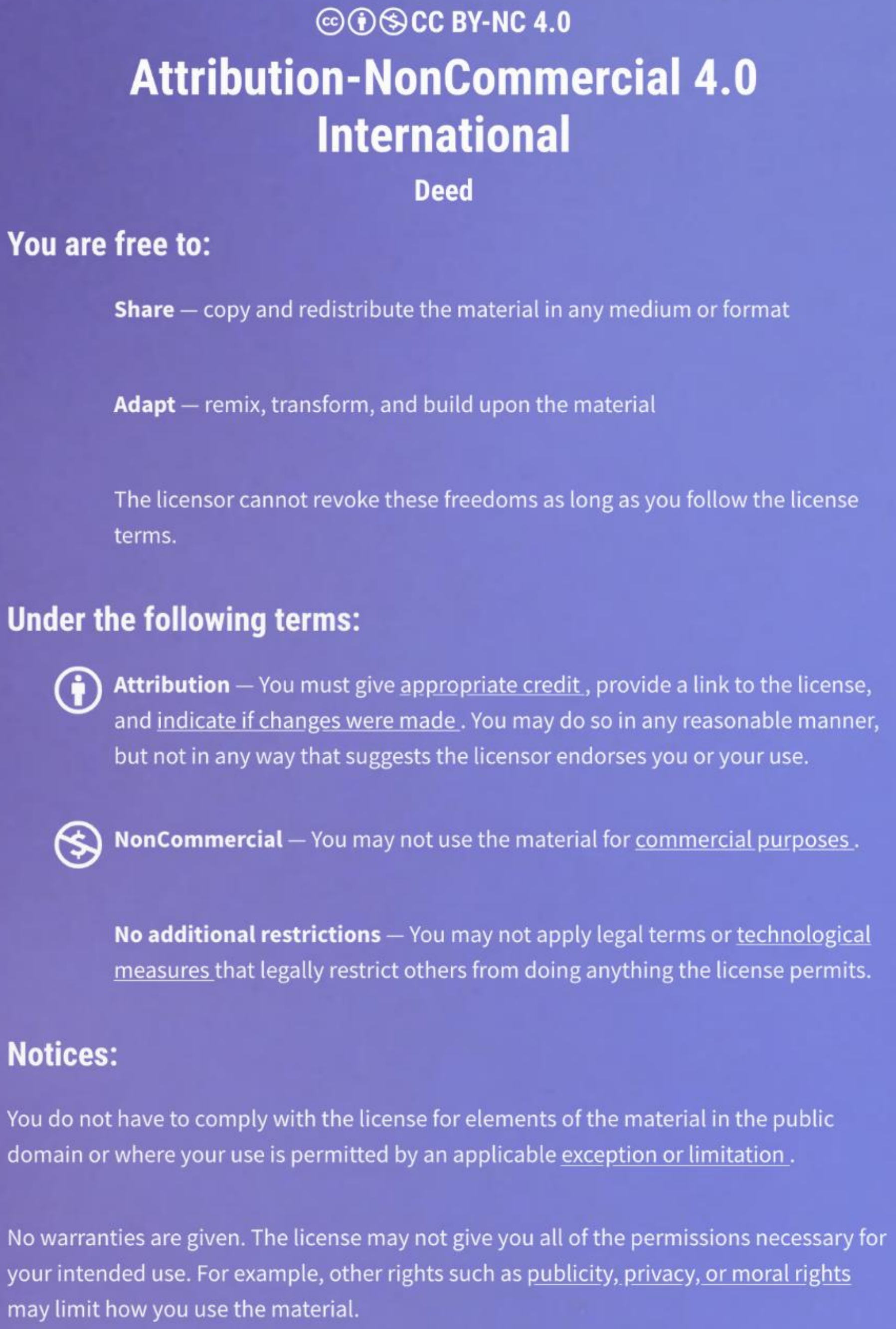
The Dead Internet & A Crisis of Perception

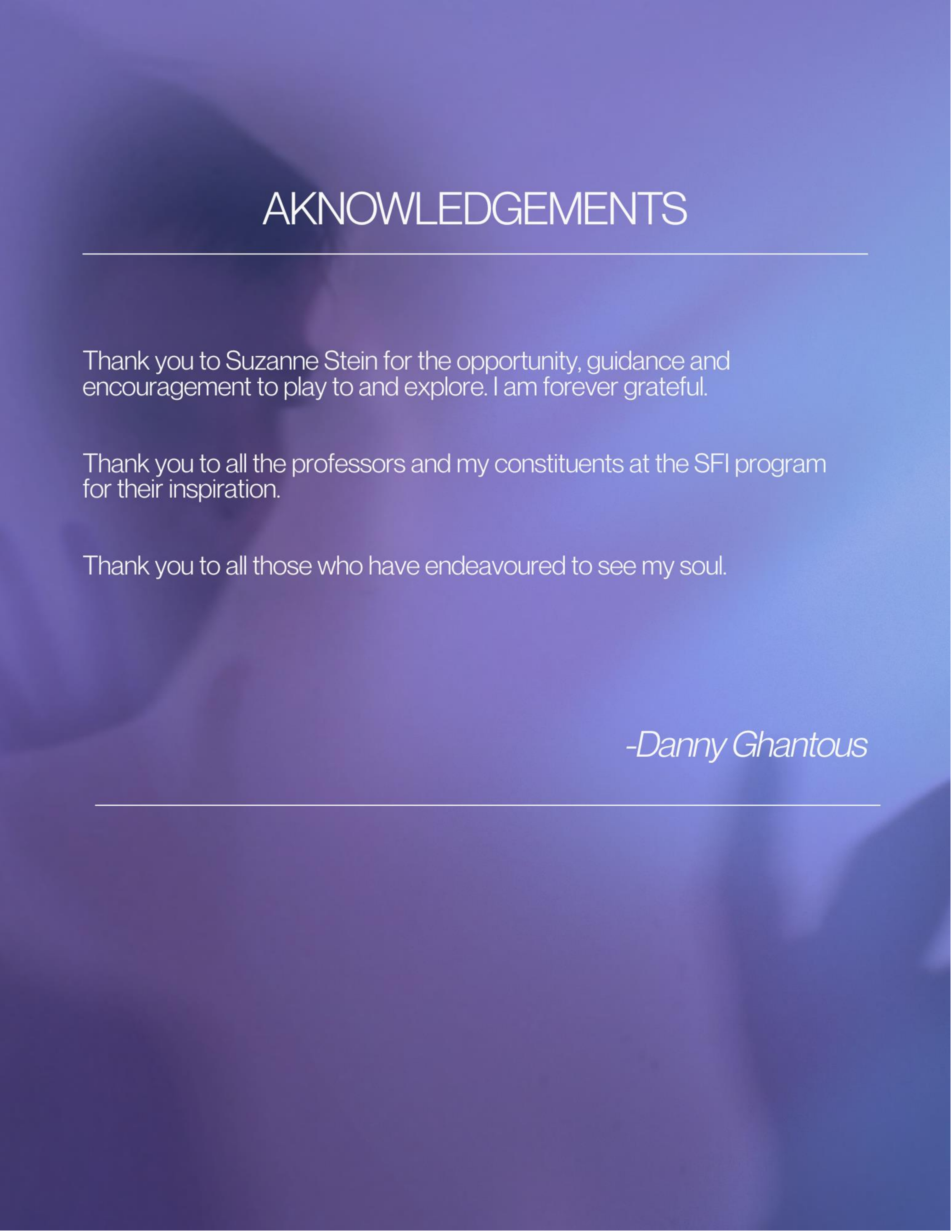
Danny Ghantous

Submitted to OCAD University in partial fulfillment of the requirements for the degree of
Master of Design in Strategic Foresight & Innovation

Toronto, Ontario, Canada, 2025

COPYRIGHT NOTICE





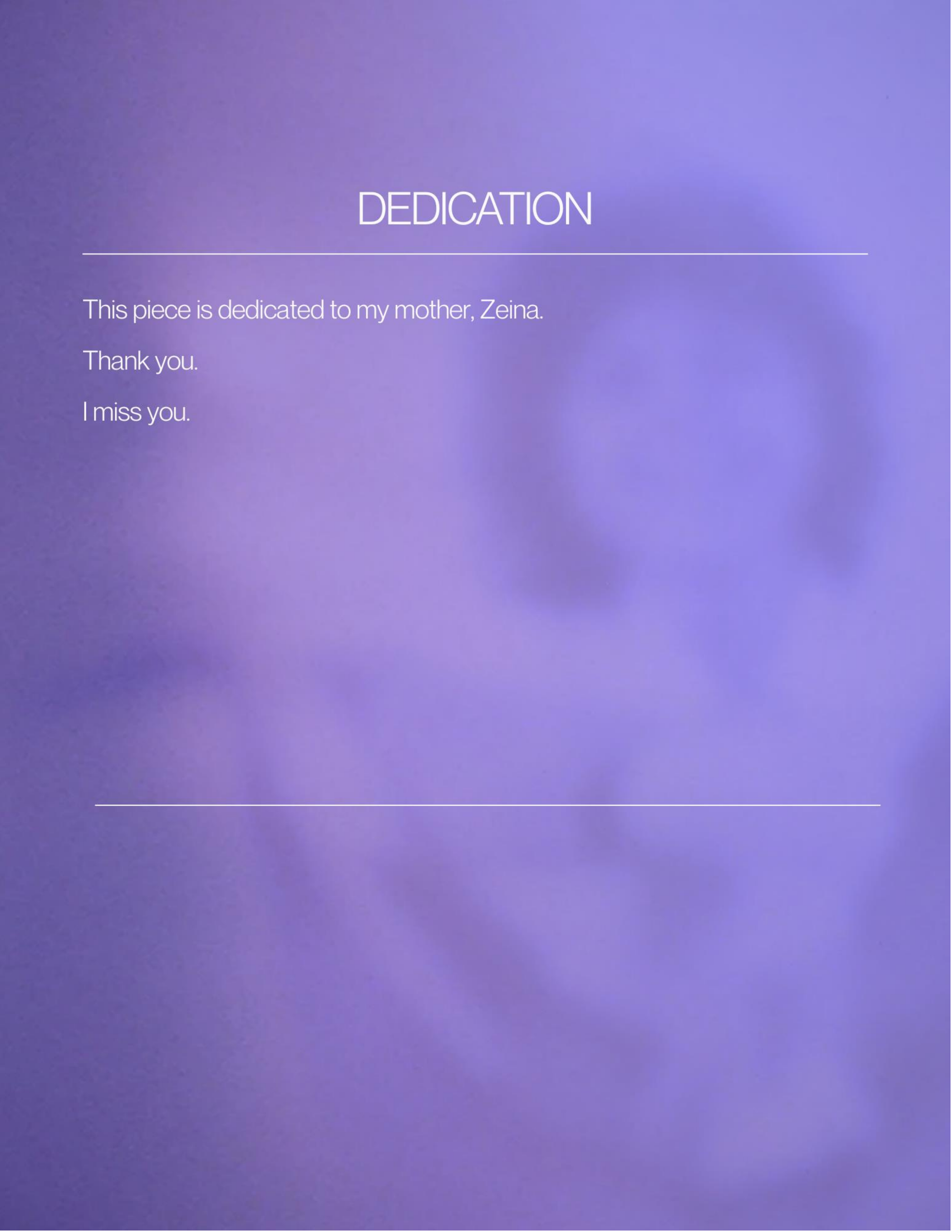
AKNOWLEDGEMENTS

Thank you to Suzanne Stein for the opportunity, guidance and encouragement to play to and explore. I am forever grateful.

Thank you to all the professors and my constituents at the SFI program for their inspiration.

Thank you to all those who have endeavoured to see my soul.

-Danny Ghantous



DEDICATION

This piece is dedicated to my mother, Zeina.

Thank you.

I miss you.

A PREFACE

I THINK I WATCHED THE MATRIX TOO MUCH AS A KID...

FOR TOO LONG, AT TOO YOUNG OF AN AGE, I MUSED ABOUT SOLIPSISM.

OF BEING NEO, CURLED UP AND FED CODE OF MY REALITY,

AND YET, WHEN I SAW THE 'WOMAN

IN THE RED DRESS' I BEGAN TO ASK,

"WHY WOULD ANYONE WANT TO

GO DOWN THE RABBIT HOLE?"

"WHY WOULD ANYONE WANT

TO LEAVE LA LA LAND?"

IF PERCEPTION IS REALITY,

WHY SUFFER?

WHY FEEL OSTRACIZED?

WHY FEEL BULLIED? UNLOVED?

WHO DOESN'T WANT A YES MAN?

WHO DOESN'T WANT UNCONDITIONAL LOVE?

A MIRROR.

THOSE WHO HAVE LIVED.

AND HAVE FOUND BEAUTY IN IMPERFECTION.

THOSE WHO RECOGNIZE THE DANCE ALL OF US PLAY, TRYING TO BRIDGE OUR SOULS.

IT'S THOSE WHO APPRECIATE ART. EXPRESSION. EMOTION. EMPATHY.

THAT WHICH MAKES US HUMAN.

IT'S BETWEEN THE LINES.

IT'S NUANCE.

IT'S LOVE.

THIS PROJECT IS TOO LARGE. IT'S TOO AMBITIOUS. IT'S TOO AMBIGUOUS.

THIS PROJECT IS AN EXPLORATION. IT'S A STORY. IT'S A WARNING.

LOOK BOTH WAYS BEFORE YOU CROSS THE INTERNET

Abstract

This study explores how widespread synthetic content and bot activity may reshape human experiences and interactions across digital and physical environments, over the next 5–10 years. Using a neo-ecological systems framework that extends Bronfenbrenner's ecological model into digital contexts, the study organizes challenges across interconnected domains, from trust formation and knowledge acquisition at the micro level across to governance and policy at the macro level. Drawing on a State of the Art (SoTA) literature review and expert interviews across a spectrum of fields, the analysis employs Reflexive Thematic Analysis (RTA) to identify emerging disruptions. Experts highlight how increasingly sophisticated synthetic entities undermine existing verification systems, distort credibility signals, outpace current governance frameworks and even threaten our shared and private epistemologies. These insights inform the foresight inquiry that follows, applying the scenario planning method through a 2x2 matrix. Structured around ten systemic change drivers, the scenarios explore four divergent futures illustrating distinct trajectories through which these challenges may unfold. This inquiry offers a set of system-level recommendations that span microsystem to macrosystem interventions, including social, technical, and policy responses. Framed in light of the "Dead Internet Theory", a once-fringe conspiracy now gaining plausibility amid the rapid proliferation of AI-driven bots, this research suggests that the mechanisms through which we establish our realities are being systematically manipulated by synthetic entities and those who deploy them, presenting a palpable, urgent and existential challenge.

Keywords: The Dead Internet Theory, bots, synthetic content, artificial intelligence, emergent technologies, human-technology interaction, foresight

TABLE OF CONTENTS

List of Tables

List of Figures

Glossary of Terms

Algorithm: A step-by-step procedure or set of rules for solving a specific problem or performing a task, particularly in computing. In digital environments, algorithms determine what content users see, how information is ranked, and how systems respond to inputs.

Algorithmic Bias: Systematic errors in algorithmic systems that create unfair outcomes, such as privileging one group over others due to flawed data or design choices.

Authentication: The process, systems, and technologies used to verify the identity of a user, device, or entity in a digital environment.

Blockchain: A distributed, immutable digital ledger technology that records transactions across multiple computers in a way that prevents retroactive alteration without consensus from the network.

Bot: An automated software program designed to perform specific tasks online without continuous human supervision. Bots can range from simple scripts to complex AI-driven systems.

Bot Network: A collection of coordinated bots controlled by a single entity or system, often used to amplify messages or simulate human activity at scale.

Cross-Contextual Verification: Verification practices that bridge digital and physical domains, using multiple methods depending on context and risk level.

Cryptography: The practice and study of secure communication techniques that protect information from unauthorized access, using mathematical concepts and protocols to encrypt data, verify identities, and ensure data integrity.

Dark Forest: Private, invitation-only digital spaces where trust is established through social verification rather than technological authentication.

Data Sovereignty: The concept that individuals or communities should maintain control over their personal data, including how it's collected, used, and monetized.

Dead Internet Theory (DIT): The belief that the internet is primarily populated by automated bots and synthetic content rather than genuine human activity.

Decentralization: The transfer of control and decision-making from a centralized entity (individual, organization, or group) to a distributed network.

Deepfake: Synthetic media in which a person's likeness or voice is digitally manipulated to appear authentic, typically created using artificial intelligence techniques.

Digital Literacy: The ability to use, understand, evaluate, and engage with digital technologies and content, including the capacity to identify misleading or harmful information.

Echo Chamber: Digital environments where users encounter only information and opinions that reinforce their existing beliefs, creating self-reinforcing information loops.

Generative AI (GenAI): AI systems capable of creating new content (text, images, audio, video) that mimics human-created content, such as ChatGPT, DALL-E, and Midjourney.

Individual Reality: The subjective cognitive framework through which a person perceives, processes, and makes meaning of information and experiences.

Infopocalypse/Infodemic: A breakdown in shared information ecosystems where distinguishing authentic from synthetic content becomes virtually impossible.

Physical Verification: Authentication methods that require in-person presence or physical interaction to establish identity or content authenticity.

Provenance: Systems that record and verify the origin and modification history of digital content to establish authenticity.

Shared Reality: The experience of having in common with others inner states about the world, fulfilling both the need for valid beliefs and the need for human connection.

Synthetic Media/Content: Digital material created partially or entirely by automated systems rather than humans, including AI-generated text, images, audio, and video.

Synthetic Entity: Automated digital actors designed to appear human or engage in human-like behaviors online, including sophisticated bots and AI systems.

Verification: Systematic procedures used to confirm identity and authenticity across digital and physical domains, specifically methods that distinguish human from non-human activity.

References for the Glossary of Terms

Note on AI, Generative AI, and Bots in This Paper:

Throughout this paper, the terms *Artificial Intelligence (AI)*, *Generative AI (GenAI)*, and *bots* may at times appear to be used interchangeably. This is not due to imprecision but rather reflects the evolving landscape in which these technological systems are increasingly interconnected.

In this context, *bots* refer to synthetic software agents that operate autonomously in digital environments, often mimicking human interaction or behavior. They function as interfaces that enable AI systems, particularly large language models (LLM's) and other generative tools, to act across platforms, engage users, generate content, and collect data at scale.

Modern AI has fundamentally transformed the capabilities of bots, making them more adaptive, human-like, and socially embedded. At the same time, bots provide the operational foundations that allows AI systems to function.

What matters in this analysis is not the precise technical classification, but the social and experiential impact of these synthetic entities and particularly how they shape human interactions on and offline.

1. Introduction

This paper investigates the growing urgency of challenges posed by synthetic content and automated systems in an increasingly bot-saturated and "dead" internet. Drawing on interdisciplinary insights from expert interviews, a SotA Literature Review, and foresight methodologies, it explores how the proliferation of bots and AI-generated content is transforming how trust, knowledge, epistemic integrity and future governance function across increasingly synthetic sociotechnical systems. Guided by a neo-ecological systems framework and extended through foresight scenario planning, this study examines emerging and potential disruptions, subsequently offering a set of system level recommendations for the general public, educators, technologists, policymakers, platforms, and institutions, aimed at fostering a more secure, trustworthy, and human-centred digital ecosystem.

The "dead internet" is not a distant dystopia. It is a burgeoning, palpable reality. As synthetic actors proliferate and information architectures degrade, we face not only a technological crisis but an epistemic one: the erosion of our ability to know, to verify, and to trust. Without innovation and intervention, we risk ceding the digital public square to algorithms and bad actors that prioritize profit over truth, automation over authenticity, and control over connection. This is not merely a crisis of infrastructure, but of intersubjectivity, where shared truths dissolve and private realities becomes increasingly malleable to synthetic influence.

1.1. Problem Statement

The internet was once heralded as a global town square and a democratizing force (Laidlaw, 2015) where humanity could connect, collaborate, and express knowledge. But today, this vision is unravelling. The internet as we know it has undergone profound transformations. Beneath the surface of our screens, bots and other products of *Artificial Intelligence* (AI) are increasingly dominating online spaces, displacing human presence on the web, and eroding the foundational trust once that sustained our digital societies and systems.

The internet has evolved from a network of primarily human-to-human communications to a complex ecosystem where human and artificial entities coexist (Walter, 2022; Imperva, 2024a). This shift, which began with web crawlers in the early 2000's, has accelerated significantly with advancements in AI and machine learning, threatening longstanding assumptions about the integrity of online interactions, the reliability of information, and the viability of the internet as a commons for democratic participation (and not just a marketplace of attention).

The concept of a "dead internet," popularized by online fringe communities in 2016, posited that bot activity had already overtaken human activity on the internet (Appleton, 2023) but was generally regarded as a conspiracy theory (Hern, 2024). However, current cybersecurity reports such as the *2024 Imperva Bad Bot Report*, reveal a startling shift: bots now account for 49.6% of all internet traffic, with malicious actors such as bot operators, attackers and fraudsters, responsible for 32% of this activity; threatening the future of human agency online and beyond, affecting not just *social* platforms, but industries from healthcare to finance to critical infrastructures (Imperva, 2024a).

The *Dead Internet Theory* (DIT) posited that much of what we currently encounter online, whether it be social media posts, product reviews, news articles, or even conversations have been manipulated by synthetic entities. The theory purports that a majority of online activity is no longer generated by humans, as it was once assumed, but rather perpetrated by sophisticated algorithms designed to mimic, manipulate, mislead and monetize (usually in that order). It warns that these bots are no longer mere nuisances. That the technology has evolved into *advanced* and *persistent* threats, capable of mimicking human behavior, evading detection, and exploiting vulnerabilities at scale (Ferrara, 2023).

With the acceleration and access to Artificial Intelligence, AI-powered bots can now simulate mouse movements, solve CAPTCHAs, and generate convincing deepfake content (Achiam et al., 2023; Huang, 2024; Imperva, 2024a; Ferrara, 2023) obfuscating the line between human and machine in the digital world (Walter, 2022) and jeopardizing our current means of detection and protection. As Yoshija Walter (2024) warns, platforms like X (formerly Twitter) and Instagram are increasingly populated by "artificial influencers": AI-generated personas that shape trends, sway opinions, and are "increasingly becoming conduits for AI-driven content, prioritizing consumption over authentic social engagement" (p. 239).

This shift is not solely technical, but existential. The internet's original promise of democratized information has given way to an epistemological crisis, in which our shared standards for truth and knowledge have fractured. Studies show that bots amplify misinformation six times faster than humans (Vosoughi et al., 2018), exploiting algorithmic biases to polarize societies and undermine democratic processes (Woolley & Howard, 2018). During the 2016 U.S. election, for example, political bots disseminated fabricated stories to millions, weaponizing engagement metrics to manipulate public discourse (Ferrara et al., 2016). Today, generative AI tools like GPT-4 enable bad actors to produce disinformation through botnets at industrial scales, while deepfake bots erode trust in visual and textual authenticity (Harris, 2023).

The implications are profound. In a 2022 Ipsos survey across 20 countries, just 63% of internet users reported trusting the internet, a drop of 11 percentage points since 2019 (Simpson, 2022). Trust is not merely *fading*; it is being replaced by a kind of *defensive skepticism*. Users increasingly question headlines, posts, and even direct messages (Walter, 2022). People now retreat into private channels and curated spaces to avoid algorithmic manipulation, a phenomenon termed digital *Dark Forests* (Appleton, 2023). Meanwhile, the economic costs of bot-driven cybersecurity breaches have surpassed $180 billion annually, and synthetic reviews are distorting entire markets (Imperva, 2024b) upending the current economic model on the internet.

This paper contends that we are witnessing a systemic breakdown, not only of digital integrity, but of the very processes by which reality is collectively shaped and socially verified. What is at stake is human agency. It is our capacity to discern, decide, and act based on signals that are trustworthy and meaningful. When those signals are manipulated at scale, and when synthetic actors shape what is seen, heard, and believed, our ability to navigate the world, online and off, is compromised.

To structure this investigation, the research organizes its analysis around a set of challenge domains identified through the initial research phase. These domains are mapped across microsystem**,** mesosystem**,** exosystem**,** and macrosystem levels, in the aims of capturing the full complexity of this emerging reality across individuals, institutions, technologies, and governance systems respectively.

1.2. Research Objectives

Considering these pressing challenges, this research seeks to address a critical primary question:

How might widespread synthetic content and bot activity reshape human experiences and interactions, both online and offline, over the next 5-10 years?

Given the complexity and emergent nature of this phenomenon across multiple domains, a *Neo-ecological Framework* has been adopted to systematically structure these topics (Navarro & Tudge, 2022). An evolution of Bronfenbrenner's Ecological systems model (Bronfenbrenner, 1979), this framework integrates *digital* environments into Bronfenbrenner's original framework, enabling the organization of sub-domains into an integrated system that acknowledges the interplay between virtual and physical contexts. Within this framework, challenge domains are distributed across four interrelated ecological levels, each representing different layers of influence on individual and collective human experience:

1. **Microsystems** (Direct Environments, Both Virtual and Physical): These are the immediate contexts where people engage with others and technologies directly. This includes interactions with bots, interfaces, and synthetic media, demonstrating how these effect:

    - *Trust Formation* (How bot interactions and activity affect trust development)
    - *Digital Literacy* (How skills for navigating the virtual world develop)
    - *Knowledge Acquisition* (How synthetic content alters learning)

2. **Mesosystem** (Interactions Between Microsystems): This level examines how different microsystems interact; for example, how online experiences impact offline decisions and vice versa. These domains include:

    - *Verification Practices* (How verification bridges online/offline experiences)
    - *Credibility Assessment* (How credibility determination spans virtual and physical contexts)
    - *Social Impact* (The boundaries and spillover between virtual and physical interactions)

3. **Exosystem** (Indirect Influences): These are the wider structures that people may not interact with directly but that profoundly affect their environments. They include:

    - *Tools and Technologies* (Technological systems, design and tools that affect user experiences)

- *Privacy and Security Systems* (How data collection and system attacks impact users)

4. **Macrosystem** (Political and Regulatory Systems): The outermost layer, encompassing the legal, institutional, and corporate governance structures that shape how synthetic actors, content and technologies are managed:

    - *Governance and Policy* (Public regulation and private standards)

Together, these challenge domains provide a structure for this inquiry, each one illuminating a specific tension, transformation, or vulnerability within an interconnected system. These domains will be further explained and explored in **Chapter 3. *Challenge Domains.***

1.3. Paper Structure

This paper is structured to investigate the challenges posed by an increasingly synthetic digital landscape through a narrative arc that connects historical developments, present challenges, and potential futures.

Following this introduction, **Chapter 2 (*The Evolution of Bots & the Dead Internet*)** establishes the historical background and foundation for the study by tracing the evolution of bot technologies from early web crawlers to contemporary AI-driven agents, examining the rise and relevance of the Dead Internet Theory, and outlining the growing palpability of synthetic entities online.

Chapter 3 (*Challenge Domains*) applies a neo-ecological framework to identify and organize the multidimensional challenges posed by bot activity and synthetic content across micro, meso, exo, and macro system levels. Each domain includes targeted subdomains, from trust formation and verification practices to tools, policies, and governance, examining the breadth of the socio-technical implications.

Chapter 4 (*Methodology*) details the research design, including the conduction of expert interviews, the Reflexive Thematic Analysis (RTA) employed to surface insights, the foresight methods used to construct plausible futures and the process for determining recommendations.

Chapter 5 and 6 (*Thematic Analysis of Expert Interviews & Perspectives from the Field*) synthesize the perspectives of expert participants through thematic codes organized by system level. These findings illustrate both converging and diverging views on the implications of synthetic activity and emerging technologies in relationship to the ascertained domains.

Chapter 7 (*Foresight*) introduces the scenario planning inquiry by identifying ten critical change drivers. Then, using a 2x2 matrix, two critical uncertainties are mapped to create four divergent futures: *Pay for Trust*, *Digital Relief*, *Dark Forests vs. the Public Internet*, and *Community Web*, to explore how these forces may influence human experiences across virtual and physical contexts over the next decade.

Chapter 8 (*Outcomes & Discussion*) reflects on key insights across the study, drawing attention to emergent tensions, existential risks, and the new epistemological conditions brought about by synthetic technologies.

Chapter 9 (*Recommendations*) builds on insights from the two preceding chapters to propose interventions across multiple systems and stakeholders. The recommendations are organized by domain and aligned with relevant actors and estimated implementation timelines.

The paper concludes with **Chapter 10 (*Conclusion*)** which offers a recap and final reflection on the implications of this research for navigating digital environments, where the boundaries between human and synthetic agency and our ability to properly discern the authentic from inauthentic continue to blur.

1.4. Framing Note

Rather than offering a traditional literature review, the following chapters: **2 (*The Evolution of Bots and the Dead Internet)*** and **3 *(Challenge Domains)***, adopt a State-of-the-Art (SotA) approach suited to research on rapidly evolving phenomena. As Barry et al. (2022) explain, SotA reviews "provide a time-based overview of the current state of knowledge about a phenomenon and suggest directions for future research" (p. 1). This framing is especially valuable for research on the Dead Internet Theory, bot proliferation and emergent technologies as it allows us to articulate, in Barry et al.'s words: "This is where we are now. This is how we got here. This is where we should go next" (p. 1). However, in the spirit of humility, and in recognition of the many plausible uncertainties and futures, this final line has been amended to reflect where we *could* go next.

The SotA review in this case is not treated as a strict methodological format, but rather as a narrative frame to orient the inquiry. It is particularly appropriate for this research as it aims to cover multiple rapidly evolving fields where the phenomena, may not be fully represented in current academic literature (Barry et al., 2022). While not a systematic literature review, the paper follows the narrative arc proposed by the SotA: beginning with synthesization of literature regarding the historical evolution of bots (capturing, *this is how we got here*) and illustrating how the digital landscape has evolved over time. The subsequent chapters, *Challenge Domains & Findings*, build on this foundation (exploring, *this is where we are now*) by mapping socio-technical tensions and risks across micro, meso, exo, and macro system levels. This framing then sets the stage for the foresight inquiry, and the recommendations that follow (addressing, *this is where we could go next*).

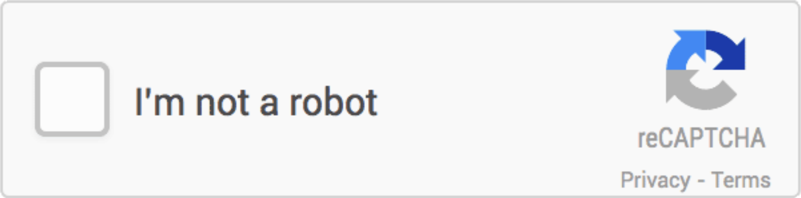
2. The Evolution of Bots & the Dead Internet: *This is How We Got Here.*

The following chapter traces the evolution of automated systems on the internet, from early web crawlers to today's sophisticated AI-driven bots. We examine how these developments have transformed what is termed the *Dead Internet Theory* (DIT) from a fringe conspiracy into a legitimate area of academic inquiry as synthetic activity increasingly dominates online spaces.

By mapping both the historical trajectory and a brief look into current challenges, this chapter creates the foundation for exploring how bot activity has and may reshape human interactions, both on and offline.

2.1. The Historical Evolution of Bots

The internet's evolution has been inextricably linked to the rise of automated software programs we have come to know as *bots*. Bots, short for "robots," are algorithms designed to perform tasks ranging from indexing web pages to now mimicking human behavior (Imperva, 2024a). Their development mirrors broader technological advancements, shifting from simple automation tools to sophisticated artificial intelligence agents, capable of reshaping online ecosystems (networks of people, businesses, and systems that use technology to interact with one another) (IMD, 2024). Understanding this progression is critical to contextualizing the DIT, which posits that human activity online has been surpassed by these bot-driven activities.



A "reCAPTCHA" checkbox, which enables web hosts to distinguish between human and automated access to websites. From Google (n.d.) at https://developers.google.com/recaptcha/docs/versions

2.1.1. Defining Bots

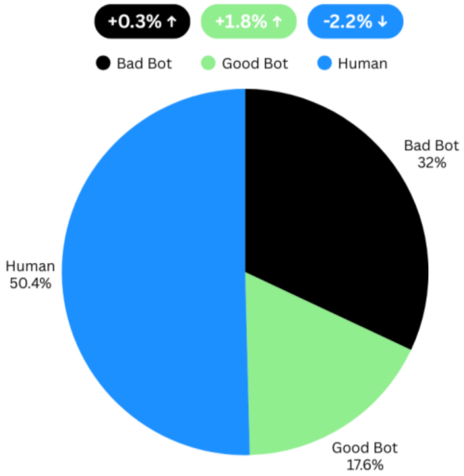
Bots are broadly categorized by intent and function. *Good bots*, such as search engine crawlers, perform essential tasks like indexing web content, monitoring site performance, or aggregating data for research (DataDome, 2022). For example, Google's web crawlers have long operated under the *Robots Exclusion Protocol*, a standard established in the 1990s to ensure ethical data collection (Koster, 1994; Koster et al. 2022).

In contrast, *bad bots* are programs thatengage in malicious activities, ranging from credential stuffing (using stolen login credentials) to content scraping (lifting content from other websites to pass as your own), and even disinformation campaigns (the intentional proliferation of falsehoods) (Radware, 2025; Imperva, 2024a). The *Imperva Bad Bot Report* (2024a), which aims to provide meaningful information about the nature and impact of bots, classifies these malicious bots into four categorizations: *Simple*, *Moderate*, and *Advanced*, with the latter two grouped as *Evasive* due to their sophistication:

1. *Simple Bots* operate using basic automated scripts from a single ISP-assigned IP address making them relatively easy to detect (Imperva, 2024a).
2. *Moderate Bots* use headless browser technology to simulate browser activity, enhancing their ability to mimic legitimate traffic (Imperva, 2024a).
3. *Advanced Bots* represent the highest sophistication, emulating human behaviors such as mouse movements and clicks. These bots utilize browser automation tools or malware embedded in browsers to bypass detection (Imperva, 2024a).
4. *Evasive bots* (Moderate and Advanced) are characterized by operators who persistently adapt tactics to evade defenses. They utilize evasive techniques such as IP cycling, anonymous or residential proxies, identity spoofing, delayed requests, and CAPTCHA circumvention. Their "low and slow" approach minimizes attack visibility, allowing them to execute impactful campaigns with fewer detectable signals (Imperva, 2024a). This adaptability and persistence make them particularly challenging to mitigate.

Figure 1

Bad Bot v Good Bot v Human Traffic 2023



Note: Bad Bot v Good Bot v Human Traffic in 2023. 32% Bad Bots (up 1.8% from last year), 17.6% Good Bots (up 0.3% from last year and 50.4% Human (down 2.2% from last year). Adapted from *The Imperva Bad Bots Report 2024*, by Imperva, 2024, p. 6, Imperva Research Labs. https://www.imperva.com/resources/resource-library/reports/2024-bad-bot-report/ Copyright 2024 by Imperva. Used under fair dealing for research and educational purposes.

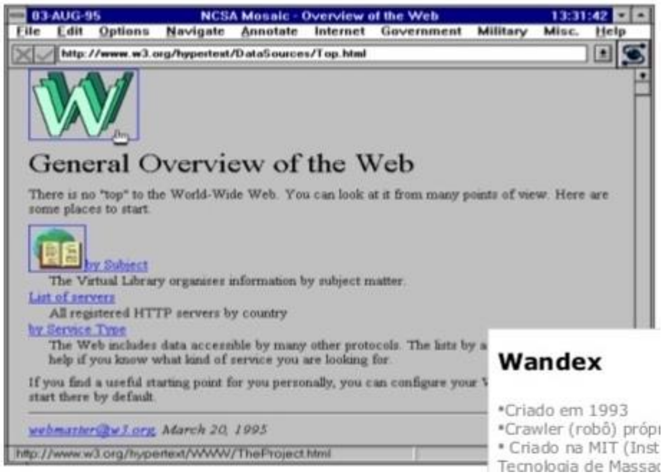
The report furthers that bad bots now constitute 32% of all internet traffic as exemplified in **Figure 1,** with sectors such as healthcare and finance disproportionately targeted due to their sensitive data (Imperva, 2024a). Operators are also utilizing these tools for increasingly malicious attacks, including the deployment of *Advanced Persistent Threats* (APT). An APT is a stealthy threat actor (often state or state-sponsored, but increasingly including non-state-sponsored groups) (Kaspersky Lab, 2021) conducting large-scale targeted intrusions that gain unauthorized network access to remain undetected for prolonged periods (Cole, 2013). These actions are primarily politically or economically motivated, and aim to steal data, conduct espionage, or disrupt operations across critical sectors such as government, defense, finance, and telecommunications (Cole, 2013). However, Imperva's report also highlights that even "good" bots can be a cause for concern:

> Good bots can significantly impact web analytics reports, as they can make certain pages appear more popular than they are. For instance, a good bot might generate an impression for a page on your website that you advertise, but that ad click never leads to the sales funnel. This can result in lower performance for advertisers and lead to skewed marketing analytics, ultimately leading to incorrect decision-making. (Imperva, 2024a, p.5)

These examples highlight the epistemic threat that even “good” bots pose within the current economic model of the web, subtly distorting perception and decision-making. To better understand how these distortions came about, it is necessary to trace the history of bots and their evolution from web crawlers to synthetic agents.

2.1.2. Early Web Crawlers (1990s–2000s)

The web’s first bots emerged as tools to organize the newly budding internet. The *World Wide Web Wanderer* (WWWW), created in 1993, was among the earliest web crawlers, mapping the internet’s growth by cataloging URLs (Gray, 1996). By the late 1990’s, search engines like Google deployed crawlers such as *Googlebot* to index pages; revolutionizing information retrieval by prioritizing hyperlink analysis (Brin & Page, 1998). These early bots operated transparently, adhering to ethical guidelines like the *Robots Exclusion Standard*, also known as “robots.txt”, which allowed website owners to control bot access (Koster, 1994; Koster et al., 2022). At this stage, bots were seen as facilitators of human-centric goals, with minimal societal disruption.



03-AUG-95 NCSA Mosaic - Overview of the Web 13:31:42

File Edit Options Navigate Annotate Internet Government Military Misc. Help

http://www.w3.org/hypertext/DataSources/Top.html

General Overview of the Web

There is no "top" to the World-Wide Web. You can look at it from many points of view. Here are some places to start.

by Subject
The Virtual Library organises information by subject matter.

List of servers
All registered HTTP servers by country

by Service Type
The Web includes data accessible by many other protocols. The lists by a
help if you know what kind of service you are looking for.

If you find a useful starting point for you personally, you can configure your
start there by default.

webmaster@w3.org March 20, 1995

http://www.w3.org/hypertext/WWW/TheProject.html

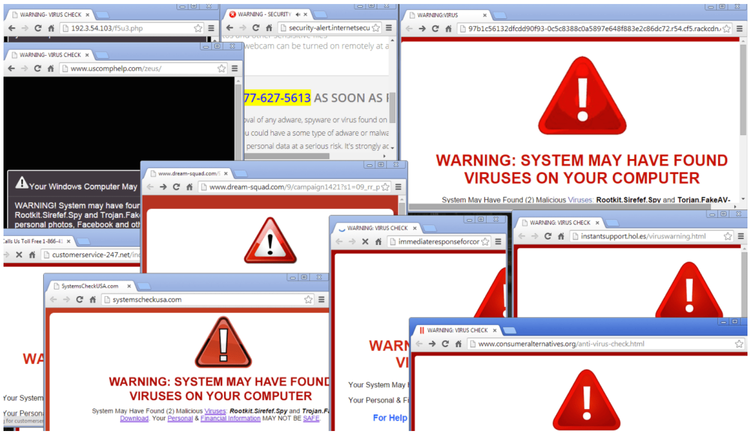
Wandex

•Criado em 1993
•Crawler (robô) própi
• Criado na MIT (Inst
Tecnologia de Massac

The WWWW was used to generate “Wandex” by Matthew Gray in 1993 as a tool to measure the size of the internet by indexing web pages. From pascu98 at https://www.timetoast.com/timelines/la-historia-de-los-buscadores

2.1.3. The Rise of Bad Bots (2000s–2010s)

As internet adoption surged, bots began to turn into tools for potential exploitation. The mid-2000’s saw the proliferation of spam bots flooding forums and email inboxes with unsolicited content, while botnets such as *Conficker* and *Zeus* hijacked devices for *Distributed Denial-of-Service* (DDoS) attacks (Cooke et al., 2005), secretly capturing passwords, account numbers, and other data used to log into online banking accounts (Federal Bureau of Investigation, 2010). In the aftermath of the 2008 financial crisis, high-frequency trading bots also emerged, as powerful market manipulators, further exacerbating economic volatility (Lewis, 2014, p.69). Researchers at this time also documented how comment spam bots were beginning to erode online discourse by exploiting cognitive heuristics (mental shortcuts and probability judgements) to manipulate user trust (Sundar et al., 2007), while simultaneously war-

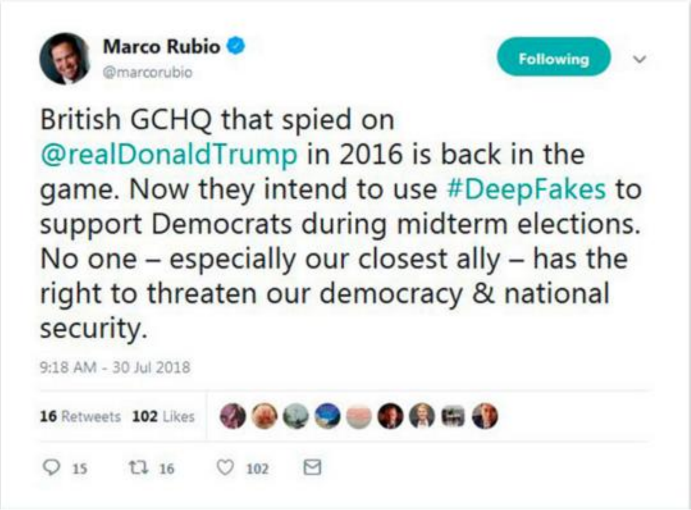


WARNING: SYSTEM MAY HAVE FOUND VIRUSES ON YOUR COMPUTER
System May Have Found (2) Malicious Viruses: Rootkit.Sirefef.Spy and Trojan.FakeAV-
Your Windows Computer May
WARNING! System may have found Rootkit.Sirefef.Spy and Trojan.Fak
personal photos, Facebook and oth
77-627-5613 AS SOON AS
WARNING: SYSTEM MAY HAVE FOUND VIRUSES ON YOUR COMPUTER
System May Have Found (2) Malicious Viruses: Rootkit.Sirefef.Spy and Trojan.F
Download Your Personal & Financial Information MAY NOT BE SAFE
For Help

Slew of pop-ups appearing due to malicious code in a virus, showing a system has been infected. From wikihow at https://www.wikihow.com/Detect-Malware ning that botnets posed greater cybersecurity threats through automated, large-scale malicious activities.

2.1.4. Social Media Bots (2010s–2020s)

The rise of social media platforms provided the ultimate fertile ground for bots to infiltrate human networks at scale. Political bots, used by regimes and actors as instruments to threaten journalists, interrupt communication amongst activists, and spread propaganda in attempts to manipulate public opinion (Oxford Internet Institute, 2016), became instrumental in disinformation campaigns, such as those during the 2016 U.S. presidential election, where bad faith actors amplified divisive content and false trends (Woolley & Howard, 2018). Ferrara et al. (2016), illustrated that *social* bots could now generate likes, retweets, and synthetic personas, mimicking human behavior to manipulate public opinion. Furthermore, reports showed that by 2017, bots produced 15% of all Twitter activity, spreading misinformation six times faster than human users (Vosoughi et al., 2018). These bots exploited algorithmic biases, funneling engagement for misinformation, and deepening societal polarization.



Marco Rubio
@marcorubio
Following

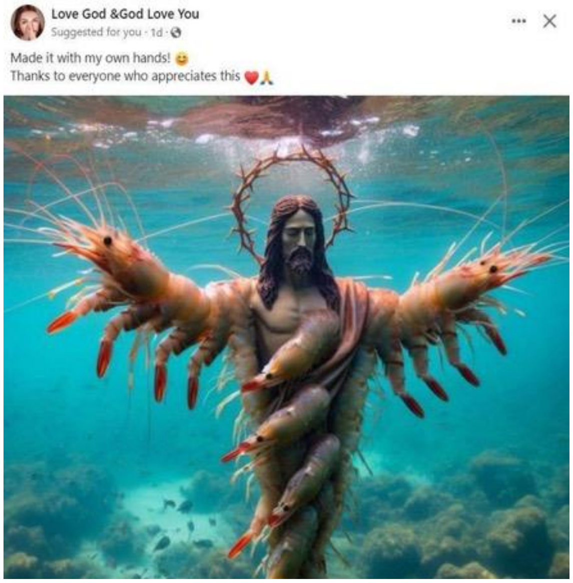
British GCHQ that spied on @realDonaldTrump in 2016 is back in the game. Now they intend to use #DeepFakes to support Democrats during midterm elections. No one – especially our closest ally – has the right to threaten our democracy & national security.

9:18 AM - 30 Jul 2018

16 Retweets 102 Likes

15 16 102

Fabricated tweet appears as if Sen. Marco Rubio is accusing British authorities of spying on President Trump. From Nimmo et al. (2020) at https://www.courthousenews.com/wp-content/uploads/2020/06/secondary-infektion-report.pdf



Love God &God Love You
Suggested for you · 1d ·

Made it with my own hands! 😀
Thanks to everyone who appreciates this ❤️🙏

"Shrimp Jesus", an AI-generated image that was part of the flood of AI-generated spam that spread throughout Facebook as a form of engagement hacking. From Farrier (2024) at https://www.web-worm.co/p/why-is-facebook-just-shrimp-jesus

2.1.5. AI-Driven Bots (2020s–Present)

Advances in generative AI such as the release of OpenAI's GPT-3, have now transformed bots into persuasive conversational agents (Radziwill & Benton, 2017) allowing them to "grasp complex human communication patterns, generating increasingly indistinguishable responses from actual human conversations" (Ferrara, 2023, p.2); while models like DALL-E and Midjourney can now generate convincing synthetic images and videos presenting novel challenges to traditional bot detection techniques, such as rule-based systems and feature engineering approaches (Ferrara, 2023).

Furthermore, the introduction of AI-powered bots has shifted from the domain of potentially nefarious actors, operating in the dark, to becoming an openly embraced strategy by companies like Meta, which is actively developing AI profiles to drive engagement amongst its users (Murphy & Criddle, 2024). This corporate embrace of artificial accounts, with Meta expecting AI characters to exist on their platforms "in the same way that accounts do" (Murphy & Criddle, 2024) further blurs the already thin line between our ability to assess the human from the artificial online.

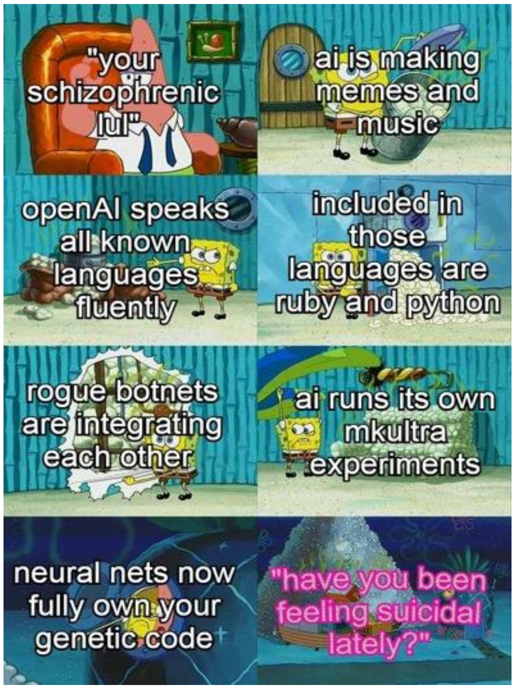
2.1.6. The Current Landscape

Today's internet is increasingly fragmented, with users retreating to closed spaces such as private Discord servers or Substack newsletters to avoid the bot-driven chaos; a phenomenon termed the *Dark Forest Theory* (Appleton, 2023). This comes as public platforms swarm with bots and fake users, with many of these accounts engaging in coordinated manipulation (Walter, 2024). However, the current scope of this phenomenon has expanded beyond the domain of the public internet. Ongoing reports affirm that malicious bots now target healthcare systems (stealing patient data), financial networks (enabling transaction fraud) and water facilities (as botnets can hijack water systems) (Imperva, 2024a; Tuptuk et al., 2021). Furthermore, current research illustrates the socio-cognitive disruptions these bots play on social cohesion, cognitive development and the distortion of reality itself (Ovadya, 2018). These developments all reinforce a significant shift in our digital and physical spaces: bots no longer merely assist or disrupt, but are actively reshaping digital ecosystems, physical infrastructures, and socio-cognitive processes. At the same time, they challenge the foundations of our *individual* and *collective* sense of reality, undermining traditional markers of trust, credibility, and security in ways that reverberate beyond the online sphere.

2.2. The Dead Internet Theory

2.2.1. Origin of the Term

The term 'Dead Internet Theory' (DIT), was thought to have emerged from online subcultures, where early adopters began questioning the authenticity of then digital ecosystems. While its precise origins remain unclear, the theory was posted to Agora Road's *Macintosh Café,* an online discussion forum, via a post entitled "Dead Internet Theory: Most of the Internet Is Fake". The anonymous author "IlluminatiPirate", along with other contributors, synthesized earlier discussions from niche communities like *Wizardchan*, where users had long speculated about the internet's "death" as early as 2016 (IlluminatiPirate, 2021). These forums, characterized by their distrust of mainstream platforms, became incubators for the theory, arguing that algorithmic content and bots had


"your schizophrenic lul"
ai is making memes and music
openAI speaks all known languages fluently
included in those languages are ruby and python
rogue botnets are integrating each other
ai runs its own mkultra experiments
neural nets now fully own your genetic code
"have you been feeling suicidal lately?"

Meme gathered from Agora Road, illustrating the escalating paranoia surrounding the DIT, showing how conspiratorial narratives evolve from skepticism to extreme claims about AI and psychological manipulation. From IlluminatiPirate at https://forum.agoraroad.com/index.php?attachments/1622441918196-jpg.3561/

overtaken human activity.

2.2.2. From Fringe to Phenomenon

The theory's development from fringe forums to mainstream outlets was initially propelled by YouTube creators and investigative journalists. A pivotal moment came with The Atlantic's 2021 article, "Maybe You Missed It, but the Internet 'Died' Five Years Ago" (Tiffany, 2021), which framed the theory as a response to post-2016 digital disillusionment.

This period also coincided with growing empirical evidence of bots dominating online spaces. By 2017, Shao et. al conducted a study on the spread of low-credibility content by bots on Twitter, and though only 6% of accounts in the sample were determined as bots, they were nonetheless responsible for spreading *31% of all tweets* linking to low-credibility content (of which, 34% of all articles proved to be from low-credibility sources) (Shao et al., 2018). Similarly, Facebook admitted to removing 2.2 *billion* fake accounts between January and March in 2019 alone (Rosen, 2019). As such, the theory's credibility and palpability by web users, grew alongside the significant advancements and public access of *Generative Artificial Intelligence* (GenAI).

2.2.3. Acceleration by Generative AI

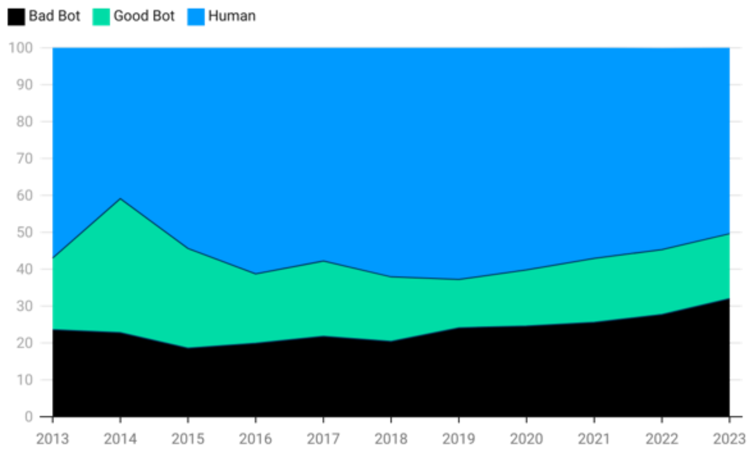
The 2022–2023 release of AI tools like *ChatGPT* and *MidJourney* marked a turning point for the proliferation of bots on the web. These technologies enabled the large-scale creation of persuasive text, images, and videos, democratizing capabilities once limited to those with technological prowess and compute access.

According to a study by Copyleaks, which offers AI-based text analysis and plagiarism services, the company "found a surge of 8,362% in AI content on the internet from November 2022, when ChatGPT-3.5 was released, to March 2024" (Copyleaks, 2024). When ChatGPT-3 was originally released in 2020, there was only a minor increase in web pages containing AI content, but since then 1.57% of some one million web pages analyzed contain AI-generated content (Copyleaks, 2024).

The *Imperva Bad Bot Report 2024* revealed that in 2023, bots accounted for 49.6% of global internet traffic, with bad bot traffic increasing for the fifth consecutive year (Imperva, 2024a). This rise is attributed to the increasing accessibility and deployment of AI-driven systems and large language models (LLMs), which lowers the barriers for automated, sophisticated activity online (Thales, 2025). As shown in **Figure 2**, the long-term trend illustrates not only the persistence of bot traffic overall, but a concerning reversal in the balance between human and automated activity online**.** The proportion of human traffic is now at its lowest level in a decade, signaling a significant shift in the composition of the web (Imperva, 2024a).

Figure 2

Bot v Human Traffic Trend from 2013-2023



Note: The chart above displays a yearly trend analysis of global internet traffic noting how automated traffic surpassed human traffic in four different years throughout a decade. Adapted from *The Imperva Bad Bots Report 2024*, by Imperva, 2024, p. 6, Imperva Research Labs. https://www.imperva.com/resources/resource-library/reports/2024-bad-bot-report/ Copyright 2024 by Imperva. Used under fair dealing for research and educational purposes..

Malicious bots alone were responsible for 32% of *all* internet activity in 2023 and Imperva (2024a) notes "how bad bots pose a grave threat to various industries and organizational functions. These bots can carry out malicious activities at a speed and scale beyond human capacity, making them a favored tool for abuse, misuse, and attacks" (pp. 9). **Table 1** outlines the wide range of industries targeted by bad bots and the specific types of attacks they most frequently encounter.

Table 1

Bad Bots by Industry

Industry	What Businesses are Included?	What Bad Bots do?
Automotive	Car Rentals, Manufacturers, Dealerships, Vehicle Marketplaces	Price Scraping, Data Scraping, Inventory Checking
Business Services	Real Estate, Third Party Vendors Like Retail Platforms, CRM Systems, Business Metrics	Attacks Targeting APIs, Data Scraping, Account Takeover
Computing & IT	IT Services, IT Providers, Services and Technology Providers	Account Takeover, Scraping
Education	Online Learning Platforms, Schools, Colleges, Universities	Account Takeover For Students and Faculty, Class Availability, Scraping Proprietary Research Papers and Data
Entertainment	Streaming Services, Ticketing Platforms, Production Companies, Venues	Account Takeover, Price Scraping, Inventory Scraping, Scalping

Financial Services	Banking, Insurance, Investments, Cryptocurrency	Account Takeover, Carding, Card Cracking, Custom Content Scraping
Food & Groceries	Food Delivery Services, Online Grocery Shopping, Food & Beverage Brand Sites	Credit Card Fraud, Gift Card Fraud, Account Takeover
Gambling	Online Gaming, Casinos, Sport Betting	Account Takeover, Odds Scraping, Account Creation for Promotion Abuse
Government	Law & Government Websites, Citizen Services, States, Municipalities, Metropolitans	Account Takeover, Data Scraping of Business Registrations Listings, Voter Registration, Appointment Scraping and Scheduling
Healthcare	Health Services, Pharmacies	Account Takeover, Content Scraping, "Helpful" Bots That Scrape for Appointment Availability
Lifestyle	Lifestyle Magazines, Blogs	Proprietary Content Scraping
Marketing	Marketing Agencies, Advertising Agencies	Proprietary Content Scraping, Ad Fraud, Denial-Of-Service, Skewing
News	News Sites, Online Magazines	Proprietary Content Scraping, Ad Fraud, Comment Spam
Retail	Ecommerce, Marketplaces, Classifieds	Account Takeover, Scalping, Denial of Inventory, Credit Card Fraud, Gift Card Fraud, Data and Price Scraping, Analytics Skewing
Community & Society	Nonprofits, Faith and Beliefs, Romance and Relationships, Online Communities, LGBTQ, Genealogy	Content and Data Scraping, Account Takeover, Account Creation, Testing Stolen Credit Cards on Donation Pages
Sports	Sports Updates, News, Live Score Services	Data Scraping (Live Scores, Odds Etc.)
Telecom & ISPs	Telecommunications Providers, Mobile ISPs, Hosting Providers	Account Takeover, Competitive Price Scraping
Travel	Airlines, Hotels, Holiday Booking	Price And Data Scraping, Skewing Of Look-To-Book Ratio, Denial-Of-Service, Price Scraping, Account Takeover, Seat Spinning

Note: In the table above, Imperva outlines the wide range of industries and specific businesses affected by bad bots, and the specific malicious activities they carry out. Adapted from *The Imperva Bad Bots Report 2024*, by Imperva, 2024, p. 41, Imperva Research Labs. https://www.imperva.com/resources/resource-library/reports/2024-bad-bot-report/ Copyright 2024 by Imperva. Used under fair dealing for research and educational purposes.

These industry-specific threats are compounded by the growing sophistication of bots themselves. Advancements in AI have significantly enhanced the capabilities of malicious bots, allowing them to evade traditional detection mechanisms and target increasingly sensitive systems.

Bots powered by tools like GPT-4 now have the means to solve CAPTCHAs (Achiam et al., 2023), evading detection systems and threatening current human verification protocols. Generative AI also simplifies the process of masking identities to bypass initial fraud checks, making it easier than ever to appear as legitimate customers or attempt fraudulent transactions, threatening our finances (Robbins, 2024). And now AI can be deployed to bypass even contemporary verification approaches such as biometric authentication systems through data breaches and even deepfaking video and voice content (Huang, 2024; Taylor, 2019; Moyo 2023). Moreover, cyberattacks are increasingly targeting critical infrastructure, including water supply systems, as evidenced by recent high-profile breaches (Rosenbaum, 2024), risking the potential for more widespread disruptions as these technologies become more sophisticated and easier to deploy. These escalations pose critical threats to traditional bot mitigation strategies and threaten users' and organizations' abilities to decipher the human from the synthetic and protect themselves from attacks. As the capabilities of bots and synthetic actors continue to advance, the Dead Internet Theory shifts from speculative hypothesis to an increasingly new normal, one that demands a deeper examination of how these forces are reshaping our interactions and understanding of reality.

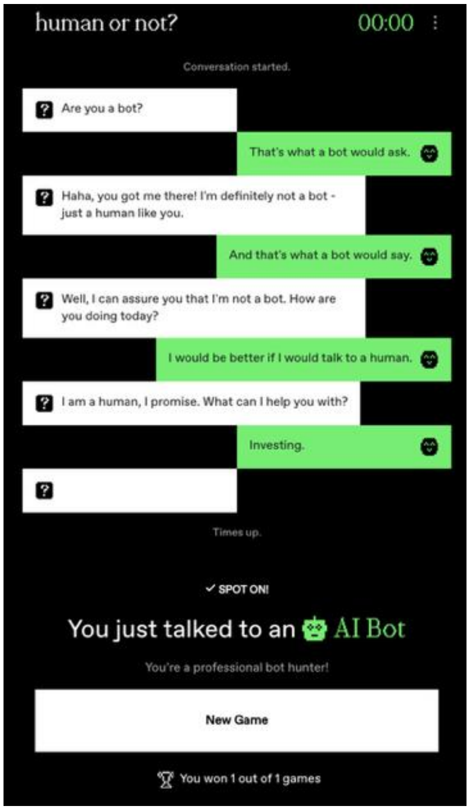
2.3. The Palpability of Bots

Although the term "dead internet" may not be as ubiquitous across internet users, nonetheless, public awareness of the proliferation of bots across the web has recently surged as users document their experience with bot activity. Such examples include:

- **Twitter 'Prompt Injection' Hacks:** By users challenging suspicious accounts on the platform to "ignore previous instructions" and providing a new task, users exploit AI powered bots attempting to mimic genuine human activity. (Edwards, 2022)

- **r/DeadInternetTheory:** A 10,000-member subreddit created in 2021 where users share personal experiences with online bot proliferation, document methods for identifying artificial content, and explore the increasingly blurred boundary between synthetic and authentic web activity.

- **Human or No**t**?:** An online game inspired by the Turing test, that measures the capability of AI chatbots to mimic humans in dialogue, and of humans to tell bots from other humans (Jannai et al., 2023). Overall users guessed the identity of their in-game partners correctly in only 68% of the games, shedding light on the inevitable near future which will commingle humans and AI (Jannai et al., 2023).



Are you a bot?

That's what a bot would ask.

Haha, you got me there! I'm definitely not a bot - just a human like you.

And that's what a bot would say.

Well, I can assure you that I'm not a bot. How are you doing today?

I would be better if I would talk to a human.

I am a human, I promise. What can I help you with?

Investing.

Times up.

✓ SPOT ON!

You just talked to an AI Bot

You're a professional bot hunter!

Screenshot of dialogue between a human user and an AI bot who accurately detects they were speaking to a machine. From The DECODER at https://the-decoder.com/humanornot-a-strangely-compelling-twist-on-the-turing-test/

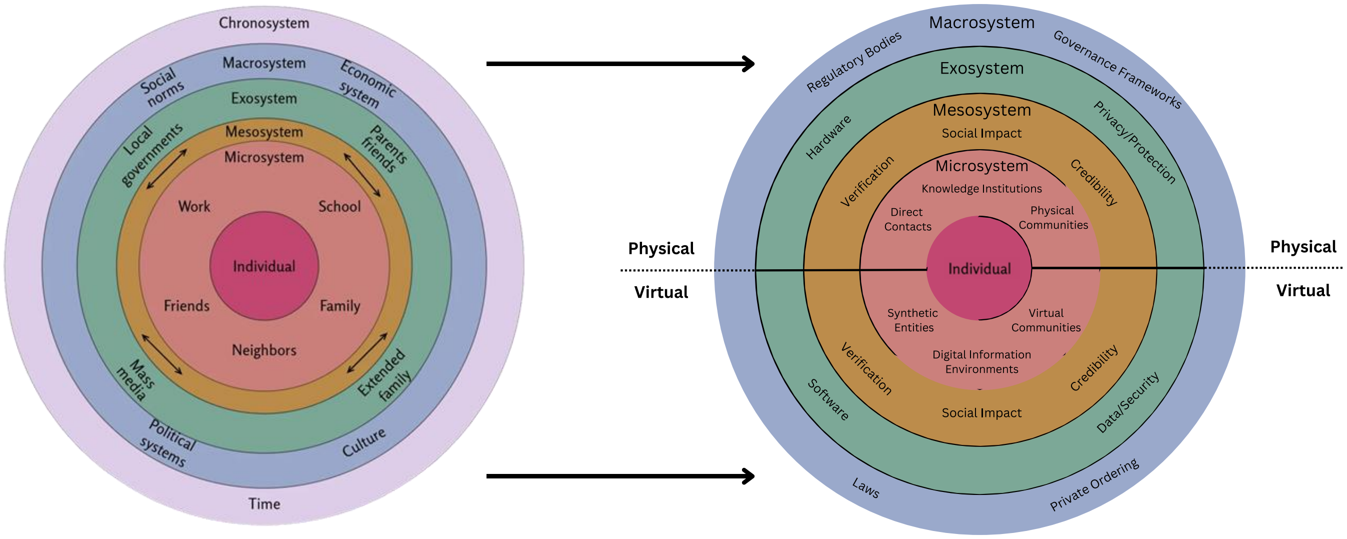
These examples underscore just a sample of how the once-conspiratorial notion of a "dead internet" has evolved into a tangible reality, where the deployment of these synthetic entities and content increasingly shape our online experiences and challenge our capacity to distinguish the genuine from the artificial.

3. Challenge Domains: *This Is Where We Are Now.*

The following section more comprehensively examines the domains affected and challenges posed by a growingly synthetic internet, drawing on academic research, industry reports and contemporary analyses from media, technology, sociology and policy discourse. Rather than isolating these challenges, we employ a neo-ecological framework, adapted from Bronfenbrenner's ecological systems theory (1979), to situate them within interconnected systems that encompass both physical *and* virtual environments. This approach provides a lens for understanding how synthetic content and bot activity reshape human experiences across multiple ecological levels, such as recognizing how 'digital literacy' extends beyond technical know-how to encompass socio-cognitive competencies cultivated in the physical world.

Figure 3

From Ecological Systems to Neo-Ecological Systems



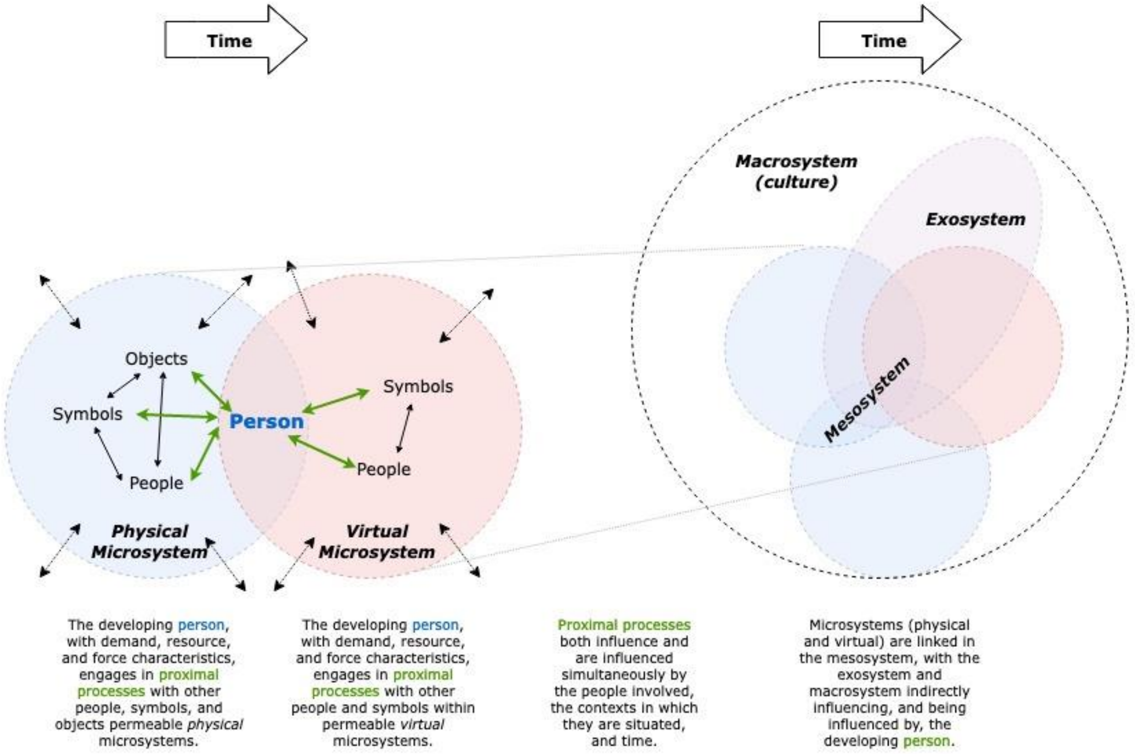
Note: This diagram compares Bronfenbrenner's original ecological systems theory, developed by SimplyPsychology (Guy-Evans, 2024) (left), with the adapted neo-ecological framework used in this study (right). The traditional model centers the individual within nested physical environments, from direct interactions to macro forces. The adapted model retains this layered structure but introduces a horizontal axis separating physical and virtual realms. Reprinted in part from *Bronfenbrenner's Ecological Systems Theory* [Online image], by O. Guy-Evans, 2024, *Simply Psychology*. https://www.simplypsychology.org/bronfenbrenner.html Used under fair dealing for research and educational purposes.

The neo-ecological framework, adapted by Jessica L. Navarro & Jonathan R. H. Tudge (2022), recognizes that in today's world, digital environments are not merely tools used within physical contexts, but rather require distinct contexts themselves, as they have their own features and influences on human development and interaction. This has been exemplified in **Figure 3** through the horizontal axis demarcating the physical realm from the virtual. Each system now explicitly includes digital facets to their physical counterparts. Microsystems now include aspects such as synthetic entities, digital environments, and virtual communities alongside physical ones. The mesosystem outlines interactions across these environments, (e.g. how virtual credibility affects physical relationships). Exosystem includes hardware/software infrastructure, data security, and privacy protection as systems shaping experience without direct interaction. Lastly, the macrosystem considers laws, regulatory bodies, and private ordering (platform governance) as determinants of digital conditions.

While the neo-ecological framework figure establishes that digital environments are equally as foundational to human experience (not just extensions of the physical), it primarily presents system levels as distinct layers. To deepen this understanding and account for the dynamics between layers, **Figure 4** adapted from Navarro & Tudge (2022) and Tudge (2008), by Sussan K. Walker (2022), illustrates how individuals navigate physical and virtual microsystems simultaneously, and how development unfolds through interactions across these systems levels.

Figure 4

Visual Representation of the Interaction between Physical & Virtual Systems



The developing person, with demand, resource, and force characteristics, engages in proximal processes with other people, symbols, and objects permeable *physical* microsystems.

The developing person, with demand, resource, and force characteristics, engages in proximal processes with other people and symbols within permeable *virtual* microsystems.

Proximal processes both influence and are influenced simultaneously by the people involved, the contexts in which they are situated, and time.

Microsystems (physical and virtual) are linked in the mesosystem, with the exosystem and macrosystem indirectly influencing, and being influenced by, the developing person.

Note: This model illustrates how individuals simultaneously inhabit both physical and virtual microsystems, with development shaped by interactions across system levels. The particular figure emphasizes the role of *proximal processes* (the ongoing processes between an individual and their environment that drive development over time) (Navarro & Tudge, 2022). Reprinted from *Visual representation of the PPCT model of neoecological theory* [Online image], by S. K.

Walker, 2022, in *Critical Perspectives on Technology and the Family*. LibreTexts. https://socialsci.libretexts.org/Bookshelves/Sociology/Marriage_and_Family/Critical_Perspectives_on_Technology_and_the_Family_%28Walker%29/02%3A_Ways_of_Understanding__Families_and_Technology/2.01%3A_Ways_of_Understanding_Families_and_Technology. Copyright 2022 by Susan K. Walker. Used under fair dealing for research and educational purposes.

Building on this neo-ecological framework, the following section introduces the challenge domains, which identify key socio-technical tensions across these system levels. These domains represent areas where synthetic content and bot activity are actively reshaping human experience and interaction at each system level:

1. **Microsystems**, which addresses immediate individual experiences in both virtual and physical environments, will examine how trust formation, digital literacy, and knowledge acquisition are transformed when synthetic activity proliferates.
2. **Mesosystem,** which explores the interactions between virtual and physical contexts, will explore verification practices, credibility assessment, and the social impact of human-bot interactions as they span both realms.
3. **Exosystem,** will focus on the technological systems and infrastructure that indirectly influence individuals, including the tools and privacy/security frameworks that shape user experiences in increasingly synthetic and insecure digital environments.
4. **Macrosystem,** will encompass and examine the broader legal, regulatory, and governance systems that define the rules and norms for synthetic content, bot activity and those who deploy them across jurisdictions and platforms.

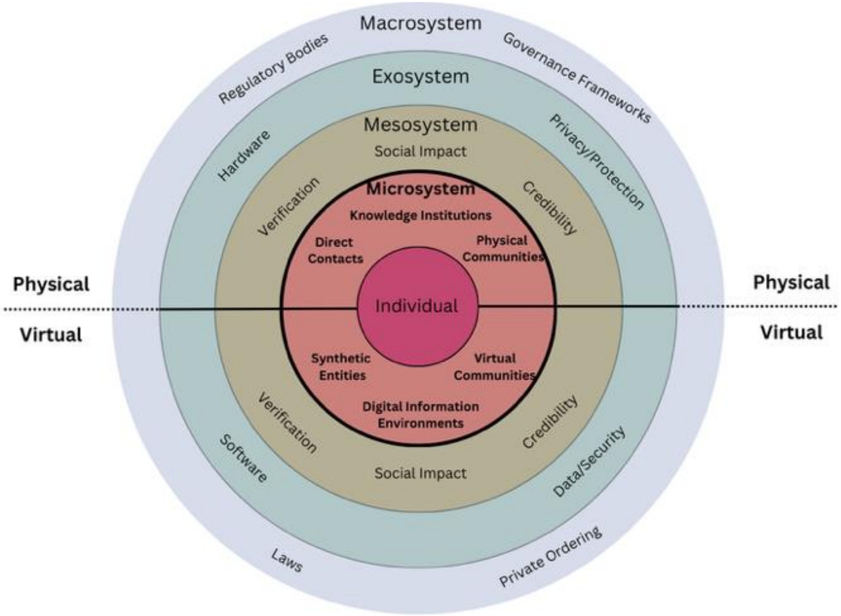
The use of this framework ultimately aims to recognize that our online and offline experiences do not exist separately but rather influence each other constantly. Furthermore, by organizing the domains in this manner, we can better order and determine the plethora of current and potential effects of synthetic content and bot activity reshaping human experiences across these interconnected domains.

3.1. Microsystem

The microsystem represents the immediate contexts in which individuals engage with and make sense of the world, both physically and digitally. In this research, the microsystem includes the most direct and personal experiences with regards to synthetic content and bot interactions, such as forming trust, our means of navigating digital environments, and knowledge formation. These domains are deeply shaped by the growing indistinguishability between human and synthetic interactions. By analyzing microsystem challenges, we investigate how bots and synthetic media might infiltrate our means of perception, cognition and trust. How they are reshaping, not only individual behaviours, but also our means of sensemaking in the digital age.

Figure 5

Microsystem Level of the Neo-ecological Framework



Note: The Microsystem level of the neo-ecological systems diagram, highlighting actors and environments across both virtual and physical realms. Adapted from Guy-Evans (2024).

3.1.1. Trust Formation

Trust serves as a fundamental mechanism that enables human interaction in both physical and digital environments. It functions as what Ting et al. (2021) describes as a *soft security mechanism*, a social concept that humans use to navigate interactions with others. In the context of this research, both physical and digital trust can be defined as a measurable belief and/or confidence that is accumulated from past experiences and represents an expecting value for the future (Ting et al., 2021). Social theories of trust, as pioneered by Simmel (Möllering, 2001) and expanded by Luhmann (Luhmann, 1982) further that trust functions as a social force that works through human association, and that performing *any* action involves uncertainty and risk, making trust necessary to function *normally* as a human, by assuming that certain risks are negligible (Luhmann, 1982, pp. 266-270). However, this concept of trust faces profound disruption in the current digital age, where synthetic content and automated agents increasingly blur the boundaries between authentic and synthetic interactions, challenging how humans establish and maintain trust in these environments. Current challenges to this notion of trust include:

- **Minimal Trust in Online Sources**: Statistics Canada published that only 13% of people trust information and news from the Internet with only 5% trusting information found on social media (Statistics Canada, 2023).
- **Global Internet Trust Decline:** Of a 20-country Ipsos survey released by The NEW INSTITUTE in 2022, the organization found that only 63% of Internet users said they trust the Internet (as a whole), which has dropped 11 points since a similar survey was conducted in 2019 (Simpson, 2022).
- **Institutional Trust Erosion:** Results from the United Nations University World Institute for Development Economics Research, show a significant decline in *institutional* trust worldwide, and the direct correlation to impacts on social cohesion, civic engagement, and perceptions of governance (Samarin, 2024)
- **AI Compounding Democratic Distrust**: Diepeveen (2024) contends that AI-generated content poses significant risks because it “accentuates and complicates wider challenges to citizens’ trust and engagement in democratic processes”.
- **Low Global Trust Index:** The Edelman Trust Barometer (2024), (a globally deployed online survey of the general population, analyzed by experts) cited that the global trust index score hit a 23-year low, with trust in governments (50%), businesses (59%), and NGOs (54%) all declining. This data underscores a *global* crisis of institutional trust and confidence.

Together this current landscape underscores the growing erosion of trust in the digital era. Specifically, it highlights the urgent need to develop strategies that restore confidence and foster social cohesion in the face of a growingly ‘dead’ internet.

3.1.2. Digital Literacy

In the context of this research, digital literacy represents a concept that encompasses both physical and virtual realms. It goes beyond the sole technical skills needed for navigating digital environments and includes the social and cognitive skills necessary to safely navigate the web. Similarly, Martin & Grudziecki (2006) identify digital literacy as, “the awareness, attitude and ability of individuals to appropriately use digital tools and facilities to identify, access, manage, integrate, evaluate, analyze and synthesize digital resources, construct new knowledge, create media expressions, and communicate with others” (p. 255). Bawden (2008, pp. 17-32) furthers that digital literacy is a framework of capabilities that enables us to thrive in digital information environments, emphasizing *critical thinking* and *evaluation skills,* rather than just technical abilities.

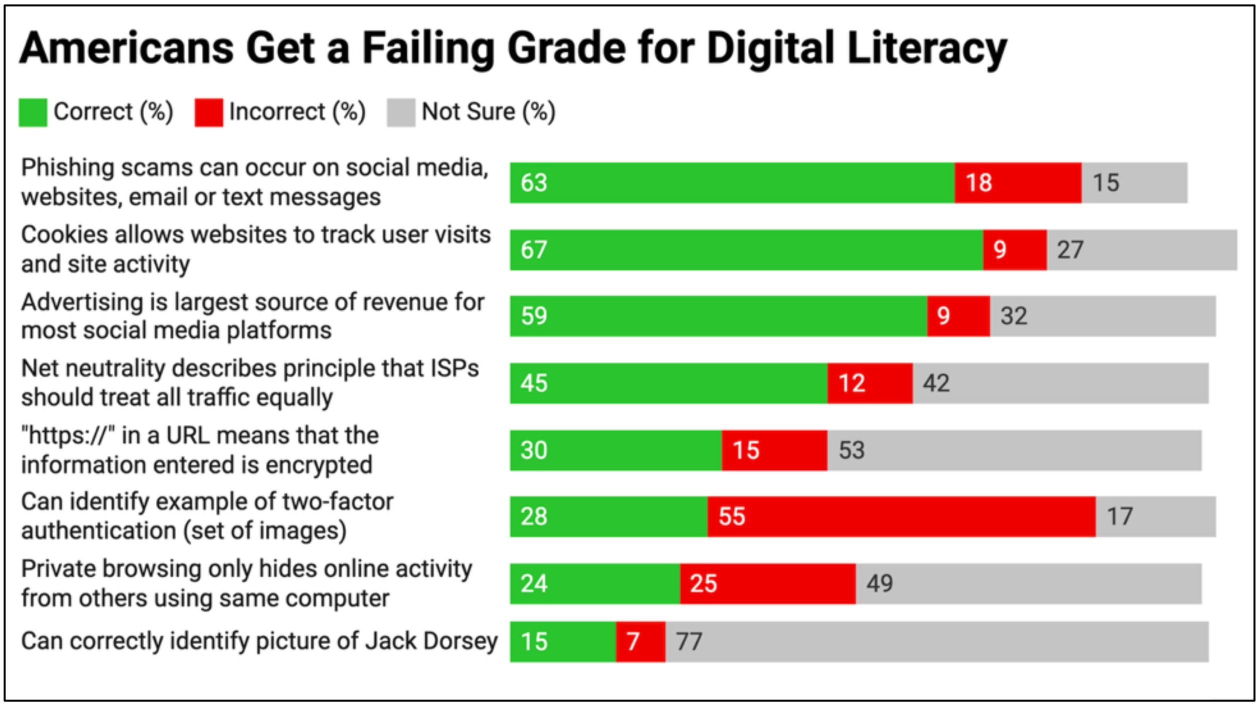
These capabilities become increasingly crucial as synthetic content proliferates across digital spaces and as they may be indistinguishable from human-created content. As such, digital literacy now encompasses the ability to distinguish between human-generated and artificially generated content.

Threats to our capacity for distinguishing synthetic from authentic activity and information have already begun to manifest in significant ways:

- **Deepfake Threats:** AI-generated deepfakes, including fake audio of public figures like former U.S. President Biden appearing to attack transgender people (Lajka 2023), are becoming indistinguishable from authentic content and reaching millions. This type of manipulation can not only affect the way the public votes, but bad actors could potentially even move the stock market with fake content of a CEO saying profits are down **(**Lajka, 2023).
- **Targeted Synthetic Deception**: During the 2020 U.S. election, studies showed that bot networks were spreading synthetic content, such as voter fraud claims, at a massive scale, specifically targeting swing states (Pratelli et al., 2023). This raises the question of the current and necessary skills and tools needed to be able to accurately assess information online, and how it affects our democratic processes.
- **Digital Literacy & American Adults**: A 2019 Pew Research Center study revealed that digital literacy remains low among U.S. adults, with respondents answering only 40% of tech-related questions correctly on average. While younger and more educated individuals scored higher, overall awareness of key digital topics such as data privacy, platform ownership, and tech policy remained limited as seen in **Figure 7** (Feldman, 2019).
- **Digital Literacy Gaps & Childhood Development**: Studies currently show that poor digital literacy skills amongst children may present significant challenges to their development. Aspects such as content risks (pornography, violence, radicalism), contact risks (cyberbullying, privacy violations), and conduct risks (fraud, misinformation) are being seen to lead to psychological problems, behavioral changes, and even physical harm to children (Gunadi, & Lubis, 2023).

Figure 6

2019 Statistics Regarding U.S. Adult Digital Literacy Competencies



Note: Pew Research Center found that U.S. adults correctly answered just 40% of digital literacy questions on average. While many recognized phishing scams and cookie tracking, deeper knowledge regarding online authentication and privacy averaged only 26% correct responses. Adapted from *What is the state of digital literacy in the USA?* by S. Feldman, 2019, *World Economic Forum*, https://www.weforum.org/stories/2019/10/americans-get-a-failing-grade-for-digital-literacy. Based on data from Pew Research Center. Copyright 2019 by Pew Research Center and World Economic Forum. Used under fair dealing for research and educational purposes.

Ultimately, as synthetic content and entities increasingly blur the boundaries between genuine and manipulated information, and as threats to digital privacy and security increase, there is an urgent need to recognize how digital literacy is not limited to a set of technical skills but rather a dynamic framework for critically navigating and interpreting our machines.

3.1.3. Knowledge Acquisition

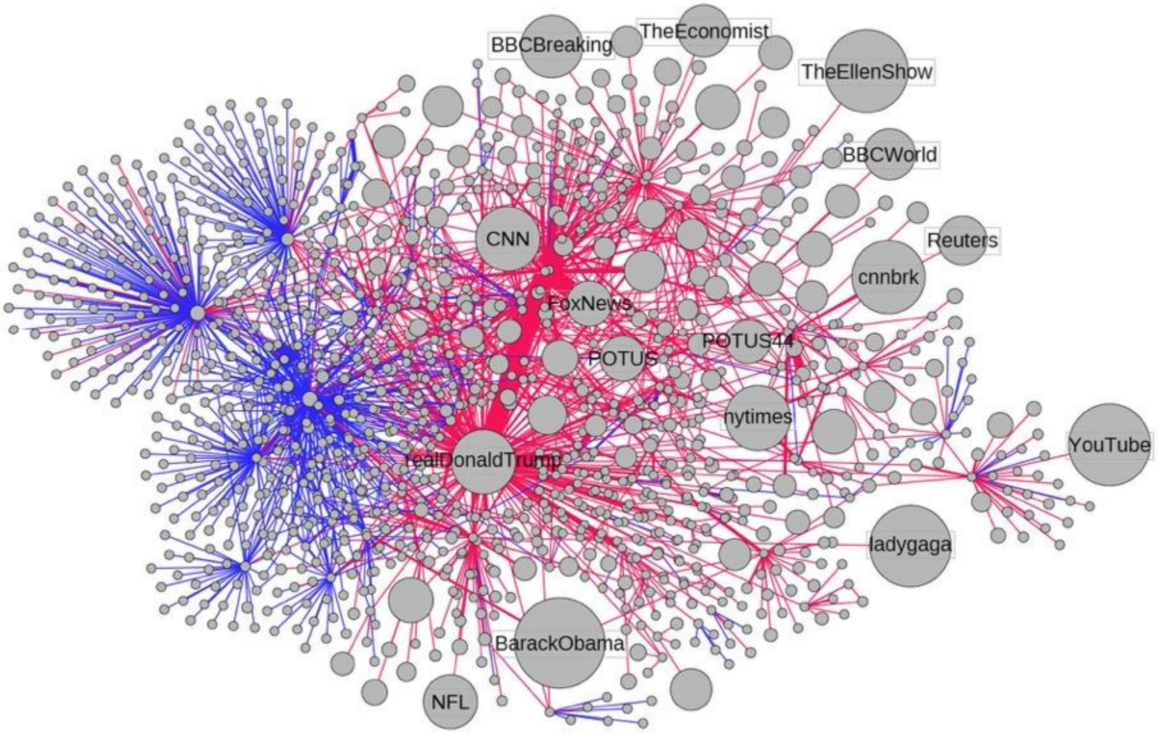
For the purposes of this research, knowledge acquisition refers to the epistemic processes by which individuals discover, internalize, and validate information, transforming it into knowledge. In both physical and virtual realms, knowledge acquisition may follow similar pathways, but digital environments introduce novel challenges to this process. As Metzger & Flanagin (2013) illustrate: “Networked digital media present(s) new challenges for people to locate information that they can trust. At the same time, societal reliance on information that is available solely or primarily via the Internet is increasing” (p.1). They further that “digitally networked communication environments alter traditional notions of trust” (p.1) in the ways by which information is discovered, validated, and introduced into existing knowledge structures.

Smith (2019) also notes that individuals rely heavily on testimony from others to acquire knowledge, making the reliability of information sources essential. Current digital environments, however, upend these relationships by introducing anonymous, synthetic, or inauthentic sources that may only appear legitimate:

- **Accelerated Misinformation Spread:** A study conducted through the MIT Media Lab in 2018 showed that bots amplify misinformation six times faster than humans (Vosoughi et al., 2018); and during the 2016 U.S. election, political bots disseminated fabricated stories to millions, manipulating public discourse (Ferrara et al., 2016) illustrating its impacts on how we discover and validate information sources online. Similarly, Shao et al. (2018) analyzed information shared on Twitter during the 2016 U.S. presidential election and found that bots played a disproportionate role in spreading misinformation online as exemplified in **Figure 8**.
- **The Retreat to Private Spaces**: In response to bot-driven chaos, Strickler (2019) & Appleton (2023) document internet users' withdrawal into digital *Dark Forests*, private digital spaces where individuals rely on networks of personally vetted sources to more reliably discover, internalize and validate information.
- **The Synthetic Barriers to Knowledge Acquisition:** Harris (2023) identifies three mechanisms through which synthetic actors impede knowledge acquisition: deception, encouraging misplaced skepticism, and interfering with our abilities to trust entities and content encountered online.
- **Algorithms Impeding Cognitive Processes**: Matta (2024) demonstrates this impediment to knowledge acquisition through the effects on “cognitive liberty,” as personalized algorithms narrow information exposure, reinforce existing beliefs, and encourage passive consumption, ultimately undermining opportunities for critical thinking development.

Figure 7

Bot Spread of Misinformation



Note: This image shows the spread of an article falsely claiming 3 million illegal immigrants voted in the 2016 U.S. presidential election. The nodes show how the article spread through replies and mentions, in red and retweets and quoted tweets, in blue. Reprinted from image by Filippo Menczer, Indiana University, as published on EurekAlert! (2021). https://www.eurekalert.org/multimedia/881720. Copyright 2021 by Filippo Menczer. Used under fair dealing for research and educational purposes.

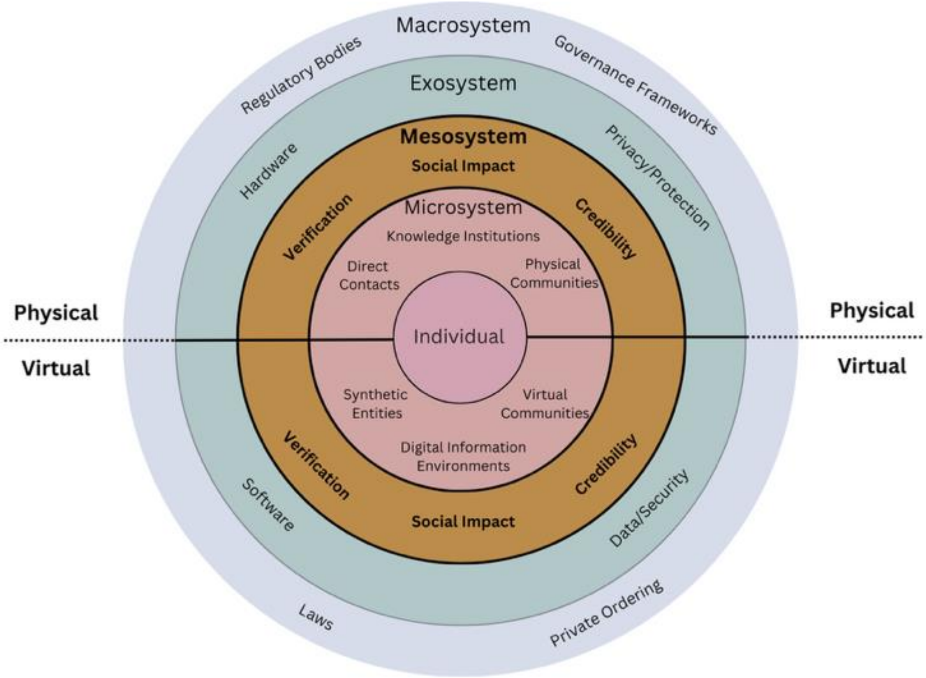
These insights reveal that digital ecosystems are not only reconfiguring the pathways of knowledge acquisition but also potentially interfering on our shared sense of reality (the experience of having in common with others inner states about the world) (Echterhoff et al., 2009). This interference occurs as narratives are increasingly manipulated, blurring the line between fact and fabrication. As a result, our capacity to establish mutual understanding is compromised, not only by misinformation itself, but by the distortion of social cues by which reality is collectively verified.

3.2. Mesosystem

The mesosystem explores how multiple microsystems intersect and how these intersections are increasingly mediated by both physical and virtual structures. In this research, the mesosystem level focuses on the relationship between people, institutions, and platforms. It investigates how verification systems function and fail, how credibility is assessed, and the social impact of human-bot interactions.

Figure 8

Mesosystem Level of the Neo-ecological Framework



Note: Mesosystem level of the neo-ecological systems diagram, illustrating how verification, credibility, and social impact operate across both physical and digital contexts. Adapted from Guy-Evans (2024).

3.2.1. Verification Practices

Verification practices represent the systematic procedures through which entities confirm identity and authenticity across digital and physical domains. In the context of this research, verification specifically refers to the methods used to distinguish human from non-human activity across the digital/physical boundary.

Historically, verification has relied on physical artifacts. As Blue et al. (2018) note, “Traditionally individuals and organisations depended on traditional paper documentation as a proof of identity, however, with technological advancements, this trend is fast becoming obsolete” (p.1). These methods were a previous means of providing assurance through *direct observation.*

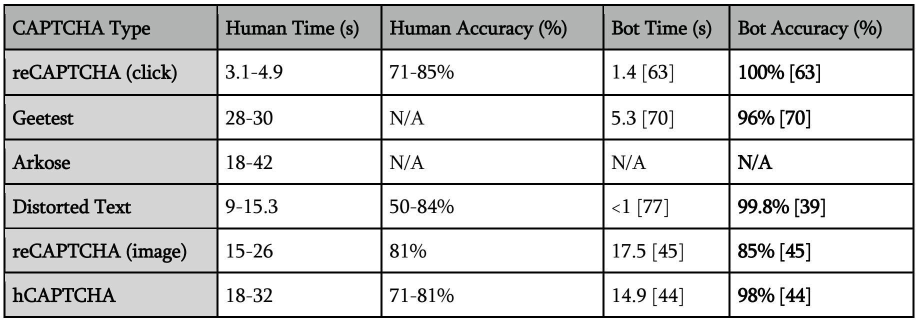
Digital environments, however, have had to develop their own approaches, described by the U.S. National Institute of Standards and Technologies (NIST) as 'identity proofing' where “an applicant provides evidence to a credential service provider (CSP) reliably identifying themselves” (Temoshok et al., 2024, p. ii). These typically relied on passwords, security questions, and device verification.

However, as sophisticated synthetic entities increasingly mimic human behavior, verification systems have begun blending physical and digital approaches. Digital systems now incorporate techniques such as biometric verification to translate physical uniqueness into digital authentication, while services such as banking or governmental services may require hybrid verification combining both digital and in-person confirmation. Yet even these blended approaches face significant challenges as the capability gap between human and machine performance has narrowed dramatically:

- **Bypassing Current Systems:** In a 2023 study, researchers found that bots often outperformed humans in both speed and accuracy when solving CAPTCHA challenges, achieving 100% accuracy on reCAPTCHA clicks and an average accuracy of 95.76%; as found in **Table 2** raising concerns about the effectiveness of current CAPTCHA systems in deterring bot activity (Searles et al., 2023, p.10). Furthermore, current AI systems can already deploy bots to bypass *biometric* authentication systems used in identity verification processes (Huang, 2024), currently thought to be a more secure means of authentication.
- **Fooling Security Experts:** Even institutions such as the cybersecurity training firm ‘KnowBe4’ mistakenly hired a North Korean hacker who utilized AI-assisted masking to create a convincing false identity through deepfake videos and forged documents (Sjouwerman, 2024).
- **Ongoing Technological Arms Race**: Researchers are already concerned with advances in quantum computing threatening to undermine emerging cryptographic security systems, highlighting the need for even more advanced protection methods (Alajmi et al., 2020).

Table 2

Humans v Bots in CAPTCHA tests



CAPTCHA Type	Human Time (s)	Human Accuracy (%)	Bot Time (s)	Bot Accuracy (%)
reCAPTCHA (click)	3.1-4.9	71-85%	1.4 [63]	**100% [63]**
Geetest	28-30	N/A	5.3 [70]	**96% [70]**
Arkose	18-42	N/A	N/A	**N/A**
Distorted Text	9-15.3	50-84%	<1 [77]	**99.8% [39]**
reCAPTCHA (image)	15-26	81%	17.5 [45]	**85% [45]**
hCAPTCHA	18-32	71-81%	14.9 [44]	**98% [44]**

Note: Table 3 compares average solving times and accuracy rates between human users and bots as reported in this study. Notably, the data shows that bots frequently outperform humans, achieving almost 100% accuracy in some fields, raising concerns about the reliability of traditional CAPTCHA systems. Adapted from Searles et al. (2023, p.10). Redistributed under Creative Commons License 4.0. https://creativecommons.org/licenses/by/4.0/

These escalating challenges signal, not just ongoing technical failures, but a deeper erosion of the mechanisms we rely on to confirm who and what is real. As verification systems increasingly blend digital and physical methods, and personal data is continuously captured and threatened, their failure becomes more than an inconvenience. When synthetic entities can continuously bypass verification systems, the reliability of verification itself comes into question. In a world where access to public services, financial systems, and even physical spaces is contingent upon successful digital verification, these failures risk excluding individuals and enabling exploitation, further destabilizing trust across both digital and physical spaces.

3.2.2. Credibility Assessment

Credibility assessment refers to the process of evaluating the believability, trustworthiness, and accuracy of information across both digital and physical contexts. While verification practices (discussed previously) focus on confirming identity and authenticity, here credibility refers to the evaluation of *information quality* and *reliability*.

Metzger and Flanagin (2013) wrestle with a contemporary definition of credibility, utilizing Aristotelian rhetorical concepts and more modern interpretations by Hovland et. al (1953) but essentially identify credibility as the believability of information sources or messages, which is assessed by individuals based on *perceptions of trustworthiness and expertise* (p. 211). We expand this concept to both physical *and* virtual information environments.

The challenge of establishing credibility is not new, but digital environments have transformed its nature. As Flanagin and Metzger (2008) further, "digital media do(es) not so much change the cognitive skills and abilities people need to evaluate credibility, as the proliferation of so much information online changes how frequently people are called upon to exercise those skills and abilities" (p.1). This leads to what Eysenbach (2008) says forces individuals to evaluate *vast* amounts of online information on their own (pp. 123-154).

Traditional credibility assessment relied heavily on established institutional authorities. As Sundar et al. (2007) explains, credibility judgments were outsourced to professional gatekeepers and regulatory agencies (pp. 367-38), who determined the frameworks of evaluation. The current digital landscape has disrupted these frameworks and powers, requiring what Lankes (2008) describes as a shift away from "traditional 'authority' methods of credibility determination, where users cede determinations to trusted third parties, to a 'reliability' approach where users seek commonalities and coherence among multiple information sources" (p.667), that is currently done so in both physical and virtual contexts.

As bot activity and content proliferates in these environments, these challenges intensify and the ability to distinguish credibility in the age of the *Infocalypse* (Schick, 2020) becomes more and more difficult:

- **Institutional Credibility Collapse:** In 2022, a Gallup poll found that Americans had experienced “significant declines” in trust in 11 of 16 major US institutions. The Supreme Court and the presidency saw the largest drops in public confidence by 11% and 15%, respectively. Trust also fell in the medical system, banks, police, public schools and newspapers as seen in **Table 3** (Aggeler, 2024; Jones 2022).
- **Lack of Faith in Expertise:** Tom Nichols, author of *The Death of Expertise* (2017) notes that “browsing WebMD puts one on equal footing with doctors, and Wikipedia allows all to be foreign policy experts, scientists, and more” and that easy access to Internet search engines “creates a pervasive distrust of expertise among the public and unfounded belief among non-experts that their opinions should have equal standing with those of the experts” (Nichols, 2024).
- **Dark Side of the Virtual Soap Box:** As bots proliferate across the web, journalists highlight that there are significant integrity challenges “because virtually anyone may publish online without gatekeepers such as publishers or editors, it is up to the recipient to assess online sources for trustworthiness and information on their credibility” (Angwin, 2024).

Table 3

2022 Gallup Poll on U.S. Institutional Trust

Institution	2021	2022	Change
	% Great deal/Quite a lot	% Great deal/Quite a lot	% pts.
Small business	70	68	-2
The military	69	64	-5
The police	51	45	-6
The medical system	44	38	-6
The church or organized religion	37	31	-6
The public schools	32	28	-4
Organized labor	28	28	0
Banks	33	27	-6
Large technology companies	29	26	-3
The U.S. Supreme Court	36	25	-11
The presidency	38	23	-15
Newspapers	21	16	-5
The criminal justice system	20	14	-6
Big business	18	14	-4

Television news	16	11	-5
Congress	12	7	-5

Note: Data adapted from a 2022 Gallup poll showing declines in Americans' trust across major U.S. institutions. The Supreme Court and presidency experienced the largest drops, alongside decreases in confidence in banks, police, public schools, and newspapers. Adapted from Jones (2022). Data found at https://news.gallup.com/poll/394283/confidence-institutions-down-average-new-low.aspx

Together, these shifts point to the current reconfiguration of how credibility is assessed in both digital and physical environments. As institutional authority erodes and synthetic content proliferates, individuals are increasingly tasked with making credibility judgments in environments where signals of trust can be easily manipulated or fabricated. In this context, credibility is has become a socially negotiated process that is prone to manipulation at scale.

3.2.3. Social Impact

Social impact, in the context of this research refers to the consequences and transformations that occur when humans interact with synthetic entities and content, with special attention to how this reshapes physical world experiences. These are the effects by which interactions with artificial agents and synthetic content alter human behaviors, relationships, and social structures.

The study of human-bot social impacts relates to the study of human-computer interaction but extends beyond a solely technological field, to encompass broader sociological impacts. As Fogg (2002) notes, computing systems can change what people think and do in ways that transcend the virtual realm. This observation has become increasingly relevant as current social bots sit at an ambiguous position between tool and agent, and synthetic content influences human behaviours on and offline.

The spillover effects from virtual to physical interaction represents a particularly important dimension of social impact. Turkle (2017) notes how technology currently "proposes itself an architect of our intimacies" describing the effect of technology on how individuals relate to each other even in purely human interactions and relationships, and the following examples demonstrate how this shaping of intimacy and interaction is already playing out in daily life:

- **Echo Chambers and Polarization**: Studies show social media bots reinforce echo chambers, where users are overexposed to content that aligns with their beliefs (Lawson, 2025). This dynamic has radicalized communities and deepened societal divides, such as the growing gender-based polarization among youth (The Economist, 2024).
- **Developmental Behavior Transformations**: Zhai et al. (2024) notes how students' over-reliance on AI, particularly generative models, affects their critical cognitive capabilities including decision-making, critical thinking, and analytical reasoning.
- **Bot-Human Relationships Affecting Human Interactions**: Walther (2025) illustrates how engagement with responsive technologies can create preference for the predictability and low emotional risk of technological relationships noting "we risk losing patience and

> empathy in our real-life relationships, where responses are not always immediate or straightforward."

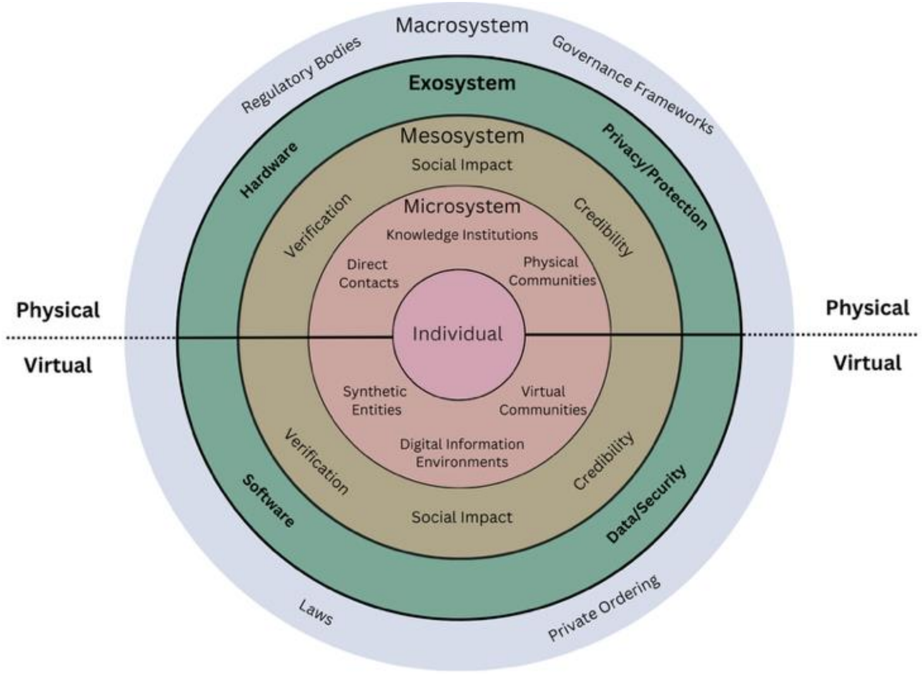
The pervasive influence of synthetic agents is not only reshaping human interactions but also transforming the very dynamics of our communities. As these digital forces manipulate information environments and deliver increasingly personalized and curated realities, they erode the shared foundations of our collective understanding. If each of us is immersed in a uniquely tailored digital world, how can we truly connect? How can we perceive the world through a common lens? These shifts force us to confront the profound consequences of a fragmented reality on both our interpersonal and societal connections.

3.3. Exosystem

The exosystem refers to the broader technological contexts that indirectly shape individual experiences and actions. In the physical realm, this includes the hardware that mediates authentication and provides the first layer of privacy protection. In digital environments, it encompasses software systems, algorithm architectures and data infrastructures. While users may rarely interact with these systems directly, their design decisions substantially influence what can be known, trusted, and/or protected.

Figure 9

Exosystem Level of the Neo-ecological Framework



Note: Mesosystem level of the neo-ecological systems diagram emphasizing the infrastructure of tools, technologies, mechanisms and systems that shape user experiences and govern information flow across both physical and digital contexts. Adapted from Guy-Evans (2024).

3.3.1. Tools & Technologies

Tools and technologies encompass the technological systems, design, and potential software solutions that shape user experiences in our increasingly bot-dominated digital environments. These are the technological advancements that enable synthetic activity, and the countermeasures used to identify and mitigate them. However, traditional tools used to identify and combat bots are narrowing in efficiency as these technologies have become more sophisticated (Alajmi et al., 2020; Huang 2024); pointing to the potential of defensive technologies failing to be able to keep apace and withstand offensive technologies.

This is already being felt through what Strickler (2019) & Appleton (2023) describe as The Dark Forest, where, as synthetic activity proliferates and efforts to manage its influence fall short, users are flocking to spaces such as Discords channels and private Slack communities, with higher barriers to entry, to preserve authentic interaction.

While blockchain-based identity systems offer promising *cryptographic solutions* (applications for securing information through the use of coded algorithms and keys, allowing only authorized parties to view the data) for verification without centralization (Gobika & Vaishnavi, 2025) and similarly, *zero-knowledge proofs* enable "a party to prove to another party that a given statement is true without revealing any additional information" (Wu et al., 2018, p.1) provide some security of authenticity, challenges, nevertheless, persist.

Contemporary bots, aided by scalable and accessible artificial intelligence can now deploy even more sophisticated countermeasures (Imperva, 2024a), creating an ongoing technological arms race that threatens to continually outpace defensive measures:

- **New Platforms, Same Bot Problems:** New Twitter alternative 'Bluesky', despite endeavouring to mimic social media's early days with "an emphasis on chronological feeds and user empowerment" (Blum, 2025), now confronts the same crisis as its predecessor: an invasion of bots that its verification systems struggle to contain (Blum, 2025).
- **One Step Ahead:** Alajmi et al. (2020) warns that current cryptographic solutions, often viewed as a crucial next step in the evolution of digital security and authentication methods, may already be vulnerable to the breakthroughs in *quantum computing* (computation that uses the principles of quantum mechanics to process information exponentially faster than classical computers) (Schneider & Smalley, 2024), presenting major security concerns for existing authentication systems

As offensive technologies grow more advanced, the gap between their ability to deploy and our ability to counteract continues to widen. The tools designed to safeguard digital spaces now risk obsolescence in the face of increasingly adaptive and scalable agents. This ongoing arms race forces us to question whether current defensive measures can ever truly outpace these technologies or if the future of our digital ecosystems will depend on fundamentally rethinking how we verify and maintain trust online.

3.3.2. Privacy & Security Systems

Privacy and security systems refer to the infrastructures and protocols that govern data collection and protection across digital environments. As Nissenbaum (2004) defines it, *privacy* represents "the flow or distribution of information" (p. 140), while *security* encompasses what Holdsworth & Kosiniski (2024) describe as "the protection of important information against unauthorized access, disclosure, use, alteration or disruption."

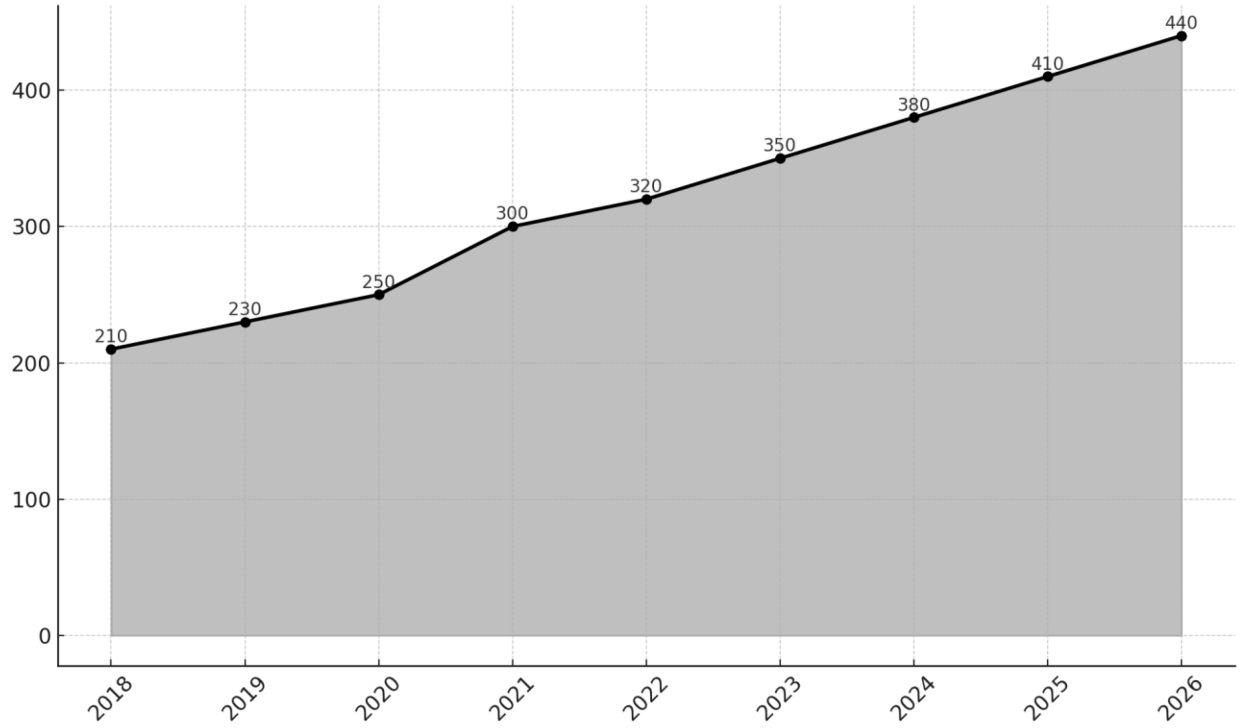
However, privacy and security have both fundamentally been transformed by the proliferation of synthetic content and increasingly sophisticated automated systems. As Solove (2008) notes, contemporary privacy challenges extend beyond simple information concealment to include issues of information processing, dissemination, and invasion. These systems operate according to what Zuboff (2019) calls “surveillance capitalism”, in which human experiences are free raw material that are translated into behavioral data and subsequently manipulated and monetized.

As synthetic activity proliferates, we observe unique challenges beyond traditional data protection, as these data systems can be exploited by automated attacks, and users exposed to its manipulation and exploitation.

- **Surge in Automated Financial Attacks:** Account takeover attacks, in which bots attempt to gain control over user accounts by exploiting vulnerabilities in authentication processes or using stolen credentials saw a 123% rise in the second half of 2022, a 108% YoY increase from the previous year (Thies, 2024). Carding attacks, in which bots use stolen credit card credentials, increased by 161%; and scraping attacks, in which bots search websites for data to be used in fraud schemes, saw a rise of 112% during the same period (Thies, 2024).
- **Data Theft & Threats to Critical Infrastructure:** Advanced bot networks now systematically probe cloud-based *Internet of Things* (IoT) systems (networks of physical objects embedded with sensors, software, and network connectivity, allowing them to collect and share data) for exploitable gaps in data transfers, taking advantage of weaknesses in their networks to intercept and collect sensitive data during transmission (Singh & Singh, 2023; IBM, 2023). These automated attacks have evolved beyond traditional methods to deploy sophisticated bot-driven ransomware campaigns, particularly targeting healthcare systems where such incidents increased by 67% from 2018-2023 and are projected to continue to increase, as exemplified in **Figure 11** (Oyekunle et al., 2025).
- **Data Vulnerabilities & Manipulation:** Song et al. (2022) highlight that the exposure and storage of identity information in verification systems has resulted in widespread security problems including “illegal use of identity, identity forging and disclosure, [and] extortion,” as evidenced by major breaches like Cambridge Analytica's unauthorized acquisition of 50 million Facebook users' data to manipulate the US election (Confessore, 2018), and the Huazhu Group leak that compromised over 100 million users' personal information (Goh, 2018).
- **Surveillance Capitalism’s Evolution:** Bot-enabled voice surveillance has transformed smart devices into continuous monitoring tools, as always-on microphones pose risks for unconsented data collection (Obermaier & Hutle, 2016, p.26). Meanwhile, monetization of behavioral data has evolved through bot-driven hyper-targeting algorithms that exploit cognitive biases at unprecedented scale (Zuboff, 2019). These synthetic systems create automated feedback loops where “predictive algorithms reshape purchasing behaviors and erode autonomy” through unrestricted access to personal data (Misra et al., 2024)

Figure 10

Projected Increase in Ransomware Incidents Over Time



Note: A predictive analysis model forecasted a continued rise in ransomware incidents, with an increase of incidents projected to hit 440 by 2026. This projection suggests that the financial and operational impact of these attacks will continue to escalate further without significant improvements in cybersecurity. Adapted from Oyekunle et al. (2025). Copyright 2025 from Oyekunle et al. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0).

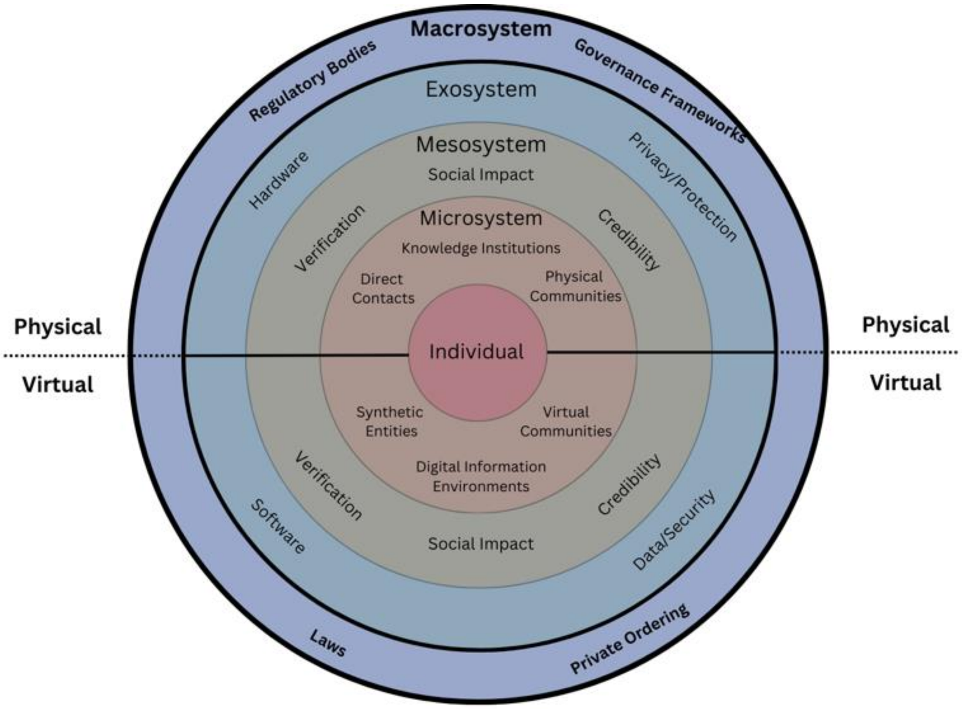
The accelerating sophistication of synthetic systems not only challenges traditional notions of privacy and security but also redefines the very landscape of digital risk. As automated entities continue to exploit vulnerabilities, the erosion of our personal control over our information becomes an increasing reality. As the extraction of our behavioural data continues, our privacy is no longer just about concealment, it is about our ability to maintain agency in a digital world where the boundaries between observer and observed continue to blur.

3.4. Macrosystem

The macrosystem encompasses the institutional, regulatory, and legal frameworks that shape the policy environments in which all other systems operate. In the digital context, this includes the governance of synthetic entities, legal enforcement, and the accountability of platforms. It also encompasses the rules and standards *self*-established by corporations, platforms, and industry bodies that function outside of formal regulation.

Figure 11

Macrosystem Level of the Neo-ecological Framework



Note: Macrosystem level of the neo-ecological systems diagram. This ring distinguishes between governance mechanisms shaping the physical (top) and virtual (bottom) realms. The top half includes *regulatory bodies* and *governance frameworks*, which typically operate through formal institutions governing physical infrastructures and public systems. The bottom half includes *laws* and *private ordering*, which more often mediate activity in digital spaces, through terms of service and platform policies. Although these entities exist physically, the split, marked by the dotted line, denotes the realm they regulate (physical or virtual). Adapted from Guy-Evans (2024).

3.4.1. Governance & Policy

Governance and policy refer to the regulatory frameworks, legal structures, and institutional approaches that currently attempt to manage digital environments as they continue to be populated by synthetic actors. This encompasses not only governmental action, but also what DeNardis (2014) calls *"private ordering"*, referring to the rules, terms of service, and content moderation policies established by private entities outside of legal frameworks.

Both legal and private frameworks represent the rules and norms that attempt to regulate behavior on the web. However, as Post & Johnson (1996) note, "the rise of an electronic medium that disregards geographical boundaries throws the law into disarray by creating entirely new phenomena that need to become the subject of clear legal rules but that cannot be governed, satisfactorily, by any current territorially based sovereign" (p. 1375). This blurs the current bounds by which any public or private entity may create, disseminate or mitigate malicious bots, let alone determine who is accountable and how responsibility is assigned for the damage done.

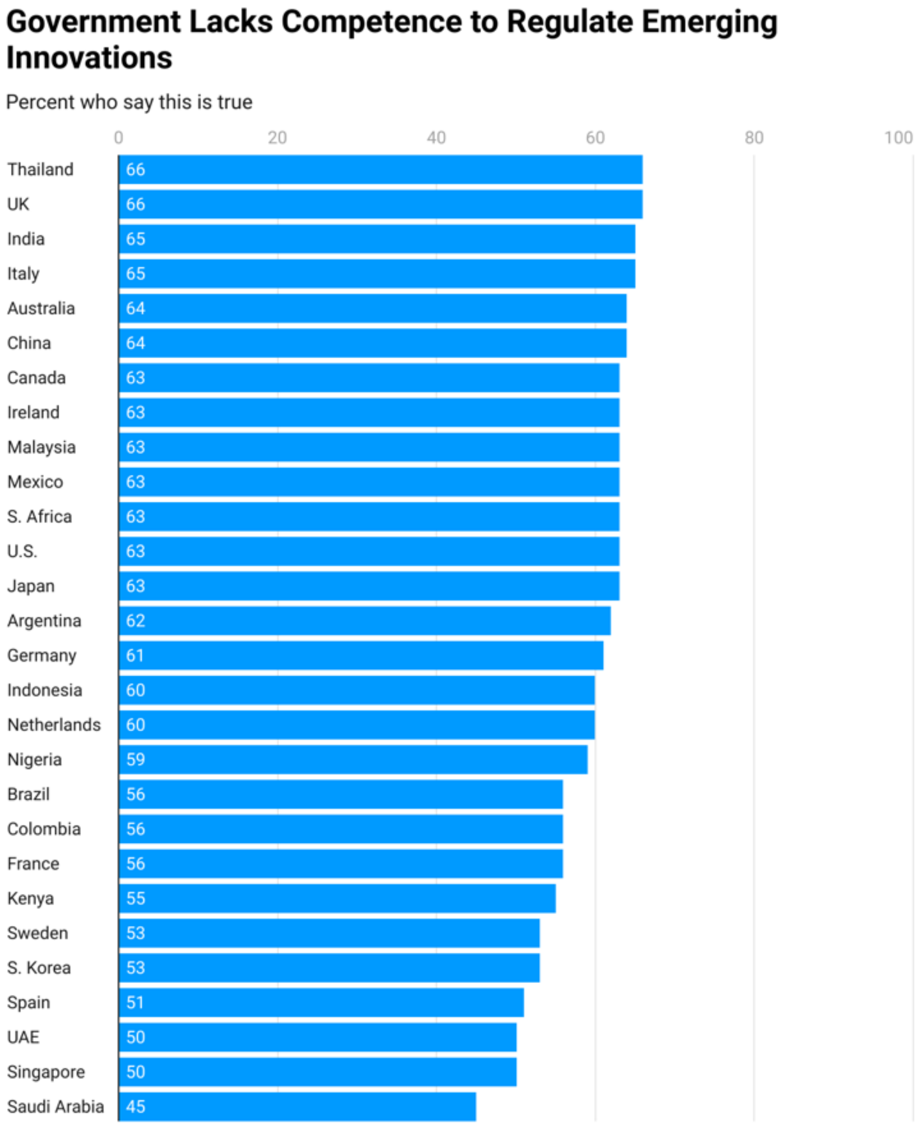
It is also important to note that industry self-regulation through technical standards bodies and professional associations attempt to bridge this gap wherein governmental regulation may be limited by jurisdiction. However, growingly sophisticated bots present novel challenges to the role of accountability for private entities crossing jurisdictional boundaries. As Citron & Chesney (2019) note concerning deepfakes, "the utility of civil suits, criminal prosecution, and regulatory actions will be limited when the source of the fake is a foreign entity that may lie beyond the reach of American judicial process" (p. 1808).

These complications are furthered by a fracturing of international governance over digital harms, and growing distrust of the governments meant to hold them to account (tension, increasingly being shaped by ongoing geopolitical divides):

- **Sovereign Intranets:** Countries like Russia and China advocate for state-controlled internet systems with content limitations, with China proposing redesigns to global internet infrastructure that would transform the open internet into a closed system where state-run providers could control citizens' internet use (European Parliament, 2024, p.9), creating fundamental challenges for the future of internet governance.
- **Regulatory Balance in the Online Harms Act:** Canada's proposed Online Harms Act (Bill C-63), aims to regulate platforms through risk mitigation plans for harmful content that can be perpetrated by bot networks, but as OpenMedia (2024) notes, while the bill appropriately targets large social media platforms and requires them to "develop and publish their own risk mitigation strategies", it also introduces concerning amendments to Canada's Criminal Code that create a type of "pre-crime" designation for individuals deemed likely to commit an online hate offense; potentially allowing restrictions on speech before activity even occurs.
- **Lack of Confidence in Government, Globally:** In the 2024 Edelman Trust Barometer, 59% of global respondents said governments are incapable of effectively regulating emerging tech, with 63% of Canadian respondents saying public officials "lack adequate understanding" to do so as exemplified in **Figure 13** (Edelman Trust Barometer, 2024).

Figure 12

Public Perception of Gov. Incompetence in Regulating Emerging Technologies



Note: This figure illustrates global perceptions of regulatory inadequacy, with 59% of respondents across 28 countries agreeing that government regulators lack sufficient understanding of emerging technologies to govern them effectively. The sentiment is strongest in countries like Thailand, the UK, and India, and remains a majority view in 26 out of 28 surveyed countries. Adapted from *2024 Edelman Trust Barometer: Global Report* (p. 16), Edelman Trust Institute, 2024. Copyright 2024 by Edelman Trust Institute. https://www.edelman.com/sites/g/files/aatuss191/files/2024-02/2024%20Edelman%20Trust%20Barometer%20Global%20Report_FINAL.pdf. Used under fair dealing for research and educational purposes.

The governance challenges posed by bot proliferation represent a critical point in the regulation of digital spaces. As bot sophistication accelerates beyond regulatory frameworks' ability to adapt, we face a significant gap in governance where neither traditional territorial sovereignty nor private ordering can effectively address cross-jurisdictional challenges and the rapidly evolving technological landscape.

4. Methodology

This chapter outlines the research methodology employed to examine how synthetic content and activity may reshape human experiences over the next decade. Given the emergent, complex, and cross-disciplinary nature of this phenomenon, the study employs adopts a mixed-methods approach that combines qualitative expert interviews with foresight scenario planning techniques to allow for both a depth of insights from specialized perspectives and the structured exploration of possible futures across multiple domains.

4.1. Expert Interviews

To comprehensively address the growing implications of the Dead Internet Theory, this study employs purposive sampling of experts across multiple disciplines. As Kallio et. al (2016) asserts, expert interviews are particularly valuable when studying emergent, rapidly evolving phenomena where traditional literature may be limited or fragmented. By synthesizing a variety of insights, the study looks beyond siloed analyses, in attempting to uncover novel problem spaces and lateral approaches to mitigating harmful bot dominance on the web.

This research particularly seeks insights beyond sole computer science or cybersecurity experts. As digital interactions increasingly shape offline social behaviors, there is growing need for input from philosophers, designers, futurists, and those involved in the policy sphere to explore the interplay between emergent technologies and human agency. Furthermore, as synthetic influencers destabilize current socio-cultural norms, perspectives from creatives and ethicists alike are needed to better understand current and potential socio-cultural impacts.

By centering multidisciplinary perspectives, this study aligns with Collet & Ciminelli's (2017) call for polyphonic analysis, which seeks to understand the tensions between voices that do not typically interplay and strives for harmony in the development of themes in qualitative research.

4.1.1. Sampling Strategy

Experts were selected through purposive sampling (Kallio et al., 2016), prioritizing individuals whose work intersects with the DIT's identified challenges:

- **Technologists and Designers**: Professionals who create, analyze, and implement technological systems and interfaces, providing critical insights on bot detection tools, AI development trajectories, and design solutions that could mitigate bot proliferation.
- **Philosophers and Ethicists**: Scholars who examine fundamental questions about knowledge, truth, and moral frameworks, offering perspectives on how synthetic content affects epistemological foundations and ethics in digital and physical environments.
- **Futurists**: Researchers who systematically explore possible futures through trend analysis and scenario development, contributing insights on long-term implications and potential adaptation strategies across multiple domains.
- **Policy-adjacent Professionals**: Individuals who analyze, develop, or implement governance frameworks, providing perspectives on regulatory challenges, jurisdictional

limitations, and potential policy approaches to synthetic activity management and public impact.

Sampling experts from diverse disciplines endeavors to gain insights across subject matter domains while mitigating bias from over-reliance on technical perspectives. Relying solely on traditional experts in technology such as computer scientists risked oversimplifying the DIT as a technical anomaly rather than a systemic societal risk. A summary of each expert's background and domain affiliation is provided in section **4.1.3** to further contextualize the analysis.

4.1.2. Potential Gaps in Perspectives

While the proposed sample captures a breadth of dimensions related to the DIT, several important gaps persist in the current research. Due to access limitations and within the project's timeframe, the following perspectives are not fully represented in the research:

- **Healthcare and Education Sectors**: Despite their vulnerability to bot-driven misinformation (Gillies, 2024; Imperva, 2024a), perspectives from medical professionals and educators are not included. These sectors face unique challenges as synthetic content targets health information and educational resources with potentially significant social consequences.
- **Legal Scholars**: The complex jurisdictional questions surrounding digital governance make legal expertise valuable, but accessing experts with appropriate cross-border data flow and sovereignty knowledge proved challenging. This gap limits the study's ability to fully assess regulatory feasibility across different legal systems.
- **Political Stakeholders**: Current policymakers could provide insider perspectives on legislative barriers, political will for technological regulation, and the practical realities of developing governance frameworks at the pace of these rapidly evolving technologies.
- **Gaming Industry Representatives**: The gaming ecosystem also represents one of the earliest domains affected by bot proliferation, with synthetic actors disrupting multiplayer environments, manipulating in-game economies, and creating new challenges for community management (Takei, 2024) threatening the potential future of online multiplayer games.
- **Environmental Scientists**: Although the environmental impacts of digital infrastructure such as energy consumption and resource consumption are well-documented, they fall outside the primary scope of this socio-technical study. The Dead Internet Theory is examined here through the lens of human-technology relations, governance, and information integrity. While synthetic activity undoubtedly contributes to growing ecological strain, this research focuses on the social, political, and technological systems that enable and respond to such phenomena, rather than their environmental externalities.

These gaps highlight the emergent nature of this phenomenon and the need for future research to incorporate sector-specific and jurisdictionally diverse perspectives to better outline potential risks and solutions across sectors.

4.1.3. Experts' Biographies

The following section presents brief biographies of the experts who participated in this study. These individuals were selected through purposive sampling for their diverse engagements with the challenges posed by synthetic content, bots, and digital trust systems. Each expert brings domain-specific insights aligned with the sampling strategy outlined above, including perspectives from technology, design, ethics, foresight, and policy. Their varied backgrounds provide the foundation for a diverse exploration of the Dead Internet Theory and the socio-technical transformations it implicates.

Daveed Benjamin: Benjamin is an American technologist holding both a BS and MS in Engineering at Stanford. He has held leadership roles in startups, nonprofits, and social enterprises in emergent fields. As a "Shift Shaper," his work focuses on altering systems of consciousness to catalyze the deep shifts that humanity urgently needs. He started work on decentralization in the early 2000s focusing on energy, food, and water and on building local economies. Now as founder of Bridgit DAO, the Presence Browser, and the Overweb and author of the book "The Metaweb: The Next Level of the Internet," his focus is decentralizing knowledge, building collective intelligence, and supporting the regeneration of the planet. Daveed is an Active Dreaming teacher, SoulCollage® Facilitator, and a Warm Data Labs host.

Keith Raymond-Harris: Harris is a postdoctoral fellow in philosophy at the University of Vienna, where they are part of the Knowledge in Crisis project. Their recent research is primarily focused on applied, social, and virtue epistemology. Their work in this area has investigated conspiracy theories, deepfakes, misinformation, epistemic vices, and so on. Their first book, entitled Misinformation, Content Moderation, and Epistemology: Protecting Knowledge, discusses the ways in which misinformation threatens the acquisition and retention of knowledge and what can be done about this. In general, their research in this area aims to identify factors that contribute to negative epistemic outcomes, and to assess potential remedies. Their research on the extended mind, and especially its connection to emerging artificial intelligence technologies, is ongoing.

Giles Lane: Lane is a storymaker – an artist, designer & researcher. They specialize in bringing creative methodologies to strategic problem-finding. Their background spans art, design and research with a focus on storymaking and designing situations that create the potential for "uncommon insight". In 1994 they founded Proboscis – a non-profit creative studio which combines artistic practice with invention and innovation, public/social engagement, commissioning, curatorial projects, design and consultancy. In 2019 they co-founded the Manifest Data Lab at Central Saint Martins, UAL as part of a 3 year AHRC-funded research project. In 2023 they joined the Royal Academy of Engineering's Policy team to lead on cross-Academy Futures & Dialogue work, including developing a new programme of public dialogue activities on 'Technology Pathways and Meaningful Innovation' towards the Just Transition to Net Zero.

Maggie Appleton: Appleton is a Lead Design Engineer at Normally, a London-based design agency specializing in early-stage AI integration for large companies. Their expertise bridges design, anthropology, and programming, with experience at companies including Elicit, HASH, and egghead. Appleton also creates illustrated essays on programming and culture; and is an advocate for expanding our use of embodied cognition and conceptual metaphors in digital interfaces. Furthermore, they contributed to "The Dark Forest Anthology of The Internet" through their piece: *The Dark Forest and the Cozy Web*, which significantly inspired and informed the current research study.

Alia ElKattan: ElKattan is an Egyptian, Brooklyn-based NYU Politics PhD candidate and creative technologist at Decifer Studio. Their research examines the political implications of the design and development of online platforms and emerging technologies. Currently they co-build interactive experiences about the impact of technology on society for broad audiences, including: The Algorithm, a Mozilla-funded simulation that demystifies social media recommendation algorithms; Survival of The Best Fit, a Mozilla-funded educational game on AI bias; and Multiplicity, a curation of articles about the internet

John Beasy: Beasy is a policy analyst and professional futurist working in the Canadian policy landscape, who holds a BA in Philosophy, Politics, and Economics from Mount Allison University. Beasy's published professional work spans governance, technological, economic, and social futures, and is currently investigating the potential shifts that artificial intelligence technologies may have across multiple policy domains; with particular focus on anticipating disruptions.

Kimberley Peter: Peter is a design and research leader with over 20 years of experience. As a researcher, foresight strategist, designer, and educator, they are guided by an interest in the leadership role of design beyond products and services and in fostering broader perspectives on the economy, growth, and innovation for the betterment of society. In addition to working with IBM, RBC, and doing independent research and consulting, they taught formally within the Digital Futures program at OCAD University and have designed and facilitated workshops on leading change, design, research, and foresight practices. They hold a Bachelor of Fine Arts in Visual Arts from the University of Lethbridge, a Master of Science in Biomedical Communications from the University of Toronto, and a Master of Design in Strategic Foresight and Innovation from OCAD University.

Karl Schroeder: Schroeder is a Canadian science fiction author, speculative designer and futurist who is currently writing about Arctic development, climate change and the future of government. Karl is best known for novels such as the award-winning YA space opera *Lockstep*, but he uses narrative tools in his foresight work as well, blending fiction with rigorous futures research in "scenario fictions" for government and corporate clients. Examples of this approach include *Crisis in Zefra* and *Crisis in Urlia*, two short novels commissioned by the Canadian Defense Department as study and research tools.

4.1.4. Expert Domains Matrix

Table 4 categorizes the experts interviewed in this research into specific domains based on their described expertise. **X** denotes primary domains, △ indicates secondary/partial professional involvement.

Table 4

Expert Domains Matrix

Expert	Design	Tech	Philosophy	Art	Futures Studies	Ethics	Politics	Banking/ Finance	Computer Science	Governance/ Public Policy
Beasy		△			X					X
Schroeder	X	△	△	X	X	△				
Lane	X	△		X	X					△
Benjamin	△	X				△		△	X	△
Peter	X	△		△	X			X		
Harris		△	X			△				
ElKattan	△	X					X		X	X
Appleton	X	X	△	X		△			X	

Note: This matrix underscores the interdisciplinary foundation of the study, highlighting the diverse lenses ranging from technology and design to policy and foresight, through which the research questions are examined.

For a more extensive detailing of the process involved regarding the expert interview questions, including the list and rationale, please refer to ***Appendix A.***

4.2. Thematic Analysis

This chapter outlines the approach employed to analyze the expert interviews conducted for this research. Reflexive Thematic Analysis (RTA) was selected as the most appropriate form of analysis given the exploratory nature of the research project, the diverse expertise of the participants interviewed and the role of the researcher as an individual; recognizing how their biases and experience effect the generation of insights.

4.2.1. Reflexive Thematic Analysis (RTA)

Reflexive Thematic Analysis, as developed by Braun and Clarke (2006), offers a flexible but rigorous approach to identifying patterns of meaning across qualitative data. Unlike other forms of thematic analysis, RTA explicitly acknowledges the active role of the researcher in the knowledge production process (Braun & Clarke, 2019). This reflexivity is particularly valuable when analyzing emergent socio-technical phenomena with a range of experts, as it allows for the recognition of multiple, intersecting interpretations.

The selection of RTA for this study was informed by several considerations. First, the diverse backgrounds of the expert participants necessitated an approach that could accommodate varied perspectives and disciplinary languages. Second, endeavouring to detail the philosophical underpinnings, epistemological positioning, and orientation provides clarity and transparency about the researcher's role and their position that: reality, knowledge production, and subjective experience are *socially* constructed.

While this approach to RTA was built upon Braun and Clarke's seminal work in their 2006 paper *Using thematic analysis in psychology*, the methodology employed here was heavily influenced by Byrne's *A worked example of Braun and Clarke's approach to reflexive thematic analysis* (2021). Byrne's paper offers an up-to-date approach to Braun and Clarke's RTA with the aim of helping to dispel some of the confusion regarding its position among the numerous other typologies of thematic analyses (Byrne, 2021).

The following sections detail the specific analytical process undertaken:

4.2.1.1. Philosophical Underpinnings

This study employs RTA (Braun & Clarke, 2006) with an *interpretivist-constructivist* approach. The interpretivist-constructivist approach assumes that reality is *socially constructed* through human interaction and interpretation, rather than existing as an *objective external reality* (William & Kouam, 2024, pp. 1-3). This approach allows for the representation of experts' attitudes, opinions, and experiences while acknowledging my interpretive role as the researcher. Furthermore, this framework recognizes that my own perspectives will inevitably influence how I understand and analyze the data.

4.2.1.2. Epistemological Positioning

The research adopts a *constructivist* epistemology, which concerns ‘how knowledge is created and understood’ (William & Kouam, 2024, pp. 1-3). This perspective recognizes language as integral to the social production of meaning and experience (Burr 1995; Schwandt 1998). Unlike *positivist* approaches that seek *objective truths*, constructivism acknowledges that meaning is created through social interactions and interpretations (Park et al., 2020).

Within this framework, codes and themes are identified based on two primary criteria as identified by the researcher:

1. **Recurrence**: Which refers to content that appear repeatedly throughout the data.
2. **Meaningfulness**: Which encompasses information that is ‘relevant’ to answering the research question and sub-topic domains, as well as subject matter deemed important by the participants themselves.

4.2.1.3. Orientation & Data Interpretation

An *experiential* orientation guides this analysis, which seeks to prioritize participants' subjective experiences (Braun and Clarke, 2014). This approach centers on meanings as described by the participants themselves, while acknowledging the social contexts that shape these meanings. Rather than deconstructing the social forces that created participants' experiences, the researcher accepts their accounts as *reflections of lived experience* (Byrne, 2021).

For a more extensive look at the thematic analysis approach, including coding, data familiarization, and generating and naming themes, please refer to ***Appendix B.***

4.3. Foresight

Following the Reflexive Thematic Analysis of expert interviews, this research employs strategic foresight methods to explore the future implications of synthetic content and bot proliferation over the next 5-10 years. Foresight methodologies offer structured approaches to anticipating developments not through precise prediction, but through systematic exploration of possible futures. This approach particularly suits exploring phenomena characterized by rapid technological development, complex interdependencies, and high stakes implications (UNDP, 2015, p.5), making it a useful tool for examining the evolving implications of what began as the Dead Internet Theory and how it may continue to unfold.

As with the RTA process detailed above, this foresight methodology acknowledges my active role as a researcher in the knowledge production process. The identification of change drivers, selection of critical uncertainties, and development of scenarios all reflect *not only* the data gathered but also *my* interpretive frameworks and disciplinary backgrounds.

4.3.1. Scenario Planning Approach

This research employs scenario planning as its primary foresight method in order to explore the potential future impacts of synthetic content and bot proliferation. Scenario planning represents a structured approach to examining possible futures that can help organizations and stakeholders prepare for various eventualities while fostering flexibility (Hiltunen, 2009).

Scenarios provide outlines of possible futures rather than predictions of a single most likely outcome. Herman Kahn, a pioneer of scenario planning, defines a scenario as “a set of hypothetical events set in the future constructed to clarify a possible chain of causal events as well as their decision points” (Kahn & Wiener, 1967, p. 6). Building on this foundation, scenarios can be understood as the description of possible futures and the course of events which allows one to move forward from the actual, to the possible future (Godet, 2000).

4.3.2. Change Driver Development

Change drivers form the foundation of this scenario planning, identifying the significant disruptive forces that shape how evolving synthetic content technologies impact various domains of human experience. In foresight, a change driver is understood as a force causing significant change to the system under study and represents “a significant disruptive force that is present in all scenarios, though it may have a different impact in each scenario” (Policy Horizons, 2024).

The development of drivers followed a process that integrated multiple data and information sources. This process included utilizing the research determined in the SotA review, identification of patterns in codes and sub-themes across the expert interviews, organization of said findings into the STEEP+V framework, and a critical assessment of *impact* and *uncertainty* levels.

Impact was assessed by evaluating the degree to which each driver could significantly disrupt the systems under this study. This included examining how a driver influences different levels of the neo-ecological framework from micro to macro levels. A driver was considered high impact if it affected multiple levels simultaneously or targeted foundational processes such as trust formation, knowledge acquisition, or reality construction.

Uncertainty was determined by examining the stability and/or predictability of each drivers’ development over time. This included evaluating how well understood the trajectory of the driver is and how susceptible it is to the rapidly changing technological, regulatory, or social environments, and the extent to which it may intersect with other drivers in unexpected or compounding ways.

This process resulted in ten key change drivers that collectively aim to illustrate the complex transformations at hand.

4.3.3. 2x2 Matrix Scenario Development

From the ten identified change drivers, two critical uncertainties are selected to form the axes for scenario development using the 2x2 matrix technique pioneered by Global Business Network and Shell (Schwartz, 1996). After careful consideration of coverage, relevance to the research question, and narrative potential, the critical uncertainties with greatest potential for generating meaningful contrasts are chosen.

These choices reflect my assessment, informed by the research study, that these two factors represent fundamental dimensions that may shape how synthetic content impacts human experience over the next decade. The intersection of these uncertainties creates four distinct scenario quadrants, each representing a possible future world.

4.3.4. Scenario Development Process

With the 2x2 framework established, each scenario is then developed through an iterative process that involves exploring the characteristics defined by the intersecting uncertainties, integrating the additional drivers, crafting compelling narratives, and identifying unique challenges and opportunities.

The resulting scenarios are tools for structured analysis, creating models of different possible futures to expand our understanding of potential developments and intervention points.

While acknowledging methodological limitations including my own temporal constraints and selection subjectivity as a sole researcher, the foresight approach employed here provides a framework for understanding potential futures that attempts to balance analytical rigor with imagination and exploration.

4.4 Recommendations

4.4.1. Recommendations Orientation

The process for the development of recommendations was grounded in a constructivist–interpretivist perspective, as has been previously outlined, which aims to recognize that the solutions proposed are constructed through *interdisciplinary sensemaking* rather than a perceived *value-neutral* analysis. In keeping with this orientation, the formulation of recommendations was approached as an interpretive process shaped by the SotA review, expert interviews, foresight exploration, and the researcher's own analytical lens. Rather than emerging from a single stage, recommendations were developed iteratively, informed by recurring patterns and tensions surfaced throughout the research project.

4.4.2. From Scenarios to Recommendations

The scenario planning process served as a central step in the formulation of the series of recommendations. The four divergent futures, developed using a 2x2 matrix, informed distinct trajectories and tensions related to verification, governance, cognition, and trust. These imagined futures provided vantage points for assessing the implications of current trajectories and exploring what interventions might be necessary and/or viable under the varying conditions of the four worlds. These tensions are further exemplified in **Appendix F.**

Initial insights emerged from both the interviews and scenario reflections. These insights were refined through cross-referencing with existing literature, ongoing technological governance initiatives and policies, and emerging advocacy efforts.

> **One such example includes:**
>
> For instance, the tensions surfaced in *Community Web*, which emphasize decentralized knowledge hubs, participatory verification, and provenance protocols mirror current discussions around provenance and decentralization. Notably, efforts such as the Coalition for Content Provenance and Authenticity (C2PA), who seek to establish provenance protocols for digital media (CP2A, 2024).
>
> However, critiques of C2PA's centralization have led to proposals from the likes of Dr. Neal Krawetz, a leader in cutting edge computer forensics research, for a more decentralized model of content authentication. As Krawetz (2024) describes, technologies such as *VIDA* employ

existing, open-source technologies to enable validation without the need for centralized authorities. This directly validated the need for initiatives such as "Decentralized Knowledge Hubs", a recommendation born directly from the *Community Web* scenario.

A table organizing these tensions and the associated broad recommendations that came about are exemplified in **Appendix G** and partially capture some of connections before refining and mapping the more specific recommendations

4.4.3. Mapping Recommendations

To translate these insights into structured recommendations, each proposal was mapped to:

- **A challenge domain**, situated within the neo-ecological systems framework (from Micro to Macrosystem)

- **A primary set of actors**, initially categorized into grouped stakeholders (e.g., Platforms, Educators, Government) and expounded upon more specifically in the recommendation itself.

- **An estimated timeline** (short, medium, or long-term), was applied, reflecting the recommendations' assumed complexity, technical readiness, and feasibility.

Figure 26 in **Chapter 9.2.1.** visualizes this mapping in an extensive Sankey diagram, illustrating the challenge domains, proposed interventions, and actor groups; and further broken down throughout the recommendations chapter by system, to help visualize these interventions better. The inclusion of timeline indicators by color coded flows also helps to distinguish between interventions that can be immediately pursued and those requiring longer term investment.

Ultimately, the recommendations composed are not fixed solutions, but exploratory pathways reflecting my interpretations, intended to provoke further design, testing, and deliberation across stakeholder communities.

5. Thematic Analysis of Expert Interviews

This chapter presents key results from our thematic analysis of expert interviews. Through analysis of interviews with the eight experts we identified consistent patterns and notable divergences in how these professionals anticipate the evolution of digital trust and human interaction in increasingly synthetic spaces.

Given the extensive nature of the full analytical results, tables of codes, themes, and synthesis matrices have been included as appendices to this report. What follows is an overview of the key themes that emerged, which will be explored in greater depth in **Chapter 6. Findings.** These themes represent the condensed insights from the extensive analysis, which is partially documented in the following appendices:

Appendix C: *Synthesis Matrix: Associated Codes and Sub-Themes by Experts Contributing to Key Themes (Anonymized)*

Appendix D: *Synthesis Matrix: Convergences and Divergences between Experts Across Themes (Anonymized)*

Note: The synthesis matrices presented in this document have been anonymized to reduce exposure and maintain a degree of discretion, despite all participants having granted explicit permission to be identified. Expert codes have been removed, and insights are synthesized at a thematic level.

At the microsystem level, our analysis revealed consistent patterns in trust cycle evolution, with experts identifying cyclical rather than linear patterns of trust adaptation. A particularly notable finding was the emergence of a trust split between general skepticism and misplaced overconfidence in synthetic content. Experts also highlighted the diminishing role of institutional trust, and the growing importance of physical reality anchoring as digital verification becomes increasingly challenging.

Within the mesosystem, experts highlighted emerging verification practices including cross-contextual verification and cryptographic approaches, while noting fundamental tensions between privacy protection and verification needs. Social impacts at this level include relationship quality transformation, changes in social skill development and evolving community formation patterns in response to synthetic content proliferation.

The Exosystem analysis revealed current and potential technological developments in bot detection systems and information architecture transformations. Meanwhile, privacy and security concerns centered on identity protection challenges and vulnerability patterns that disproportionately affect vulnerable and marginalized populations.

At the macrosystem level, governance approaches revealed divergence among experts, with competing visions of regulatory, market-driven, and community-based solutions. Experts also consistently identified power asymmetry issues related to computational access and power, and on the implementation timelines needed or expected for effective responses.

6. Findings: *Perspectives from the Field*

The following section presents findings from expert interviews, structured through the neo-ecological framework. Each challenge domain draws on a reflexive thematic analysis of coded interview data. The analysis revealed both convergences where experts shared common understandings of challenges and possible solutions, and divergences where they offered contrasting perspectives on the nature, severity, and appropriate responses to the DIT.

To visualize how expert responses clustered around specific ideas, each domain includes a figure showing the proportion of codes that contributed to key sub-themes. These sub-themes emerged during analysis and reflect significant patterns based on recurrence and/or meaningfulness. Together, the figures and accompanying insights capture how experts understood and anticipate responses to the rise of synthetic content and entities.

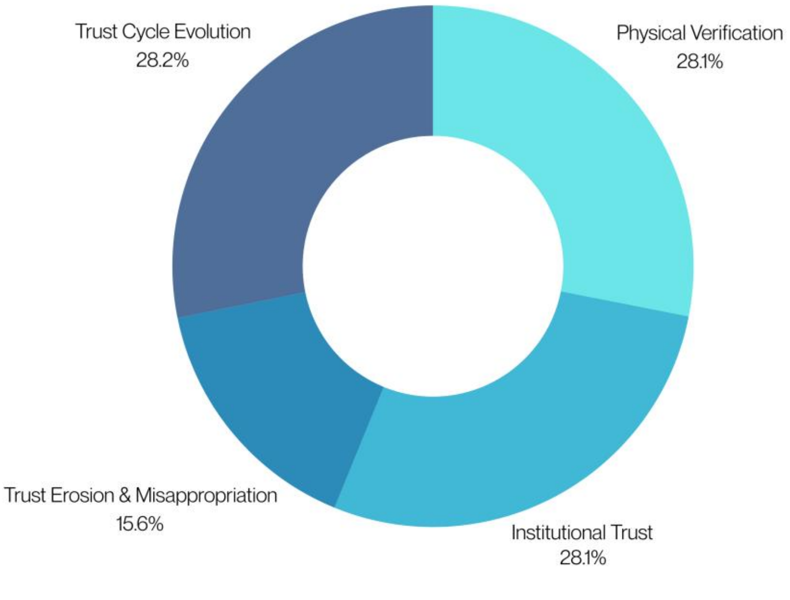
Note: Unless otherwise cited with a full reference, quotations in this chapter (e.g., *Last Name [Year]*) are drawn from the expert interviews conducted as part of this research study. As these interviews are not publicly accessible, they are not included in the reference list. For more context on the interview participants, see **Chapter 4.1.3**. *Expert Biographies* and **Chapter 4.1.4.** *Expert Domains Matrix*. Quotations from published works are cited conventionally and appear in the reference list.

6.1. Trust Formation

The expert interviews revealed a current transformation in trust dynamics within increasingly synthetic digital environments, subsequently effecting trust formed offline. Rather than simply eroding linearly, experts outlined how trust appears to operate in cyclical patterns of disruption and adaptation.

Figure 13

Trust Formation Distribution Chart



Note: Distribution of expert codes within the domain of Trust Formation including trust erosion generally and institutionally, the use of physical verification methods and the concept of “trust cycles”.

Several experts emphasized that trust, particularly in technological systems, tends to evolve in cycles marked by innovation, breakdown, and recovery. Harris (2024) noted that “There will probably be some more innovations that then undermine those verification systems, so I would imagine that there's going to be a sort of cycle to this.” Lane (2024), reinforced this concept through describing how “throughout history where we've allowed automation to totally overtake in other industries and other areas of life, it has always led to some form of collapse” followed by eventual remediation, typically operating on “a 30-to-40-year cycle.” These cycles involve periods of over-optimistic implementation, followed by an eventual collapse, and finally rebuilding with improved systems. Beasy (2025), focused on the technological aspects of these cycles, describing how verification failures lead to trust collapse, while Harris (2024) characterized it as an ongoing “arms race” between detection and spoofing technologies where neither side maintains advantage for long.

This cyclical nature is now accompanied by what some experts highlighted as a concerning “trust split”; where skepticism toward legitimate sources develops alongside a dangerous overconfidence in certain synthetic or alternative sources. ElKattan (2024) highlights this threat, claiming there is “an erosion of public trust in general... but the other direction that I think it could go into is creating disproportionate trust in actors that you shouldn't be trusting.” This split can be seen in members of the public seeking out and aligning with alternative news sources, such as Infowars, or the rise of “influencers as journalists” (Maddox, 2024). This is developing what Appleton (2024) characterizes as an “epistemic crisis” where distinguishing credible from non-credible sources becomes increasingly difficult regardless of individual digital literacy.

Experts also identified how institutional trust faces particular challenges in this landscape. They highlighted how society appears to be transitioning from *cautious institutional trust* to *normalized institutional skepticism*, affecting both private and public bodies. ElKattan (2024), specifically emphasizes government accountability concerns, noting “we need government regulation for government actors as well”, as state actors themselves deploy bots to manipulate information ecosystems. This decline in perception of trust for larger institutions reinforces the ‘trust split’ discussed earlier, as members of the public, losing trust in their institutions, seek voices outside traditional authorities.

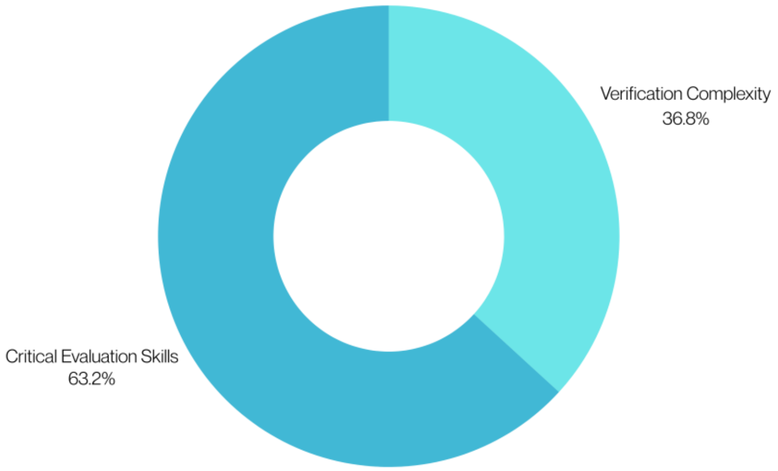
Perhaps most striking is what experts identified as a possible reversion to physical verification as digital trust mechanisms fail. As Appleton (2024) observes, “We have no way for old school institutions to confirm identity anymore, except for showing up in person.” This represents a profoundly ironic circular evolution where advanced digital technologies push us back toward pre-digital verification methods, relying on what Appleton calls a “ring of trust where meeting in physical space validates people” (2024) and may even extend to validating information by what Schroeder (2025) calls “Physical Auditing”, where members of communities may be sent to validate news stories in-person.

6.2. Digital Literacy

The interviews consistently highlighted the critical challenges currently and potentially facing digital literacy in increasingly synthetic information environments. At the core of this challenge experts identify the urgent need for new cognitive skills that extend beyond current traditional digital literacy capabilities to specifically address how to properly evaluate synthetic content and actors.

Figure 14

Digital Literacy Distribution Chart



Note: Distribution of expert codes within the domain of Digital Literacy including *Critical Evaluation Skills* and *Verification Complexity.*

The experts converge on the necessity of expanding digital literacy beyond basic technical skills, emphasizing the need for critical capacities that can meet the demands of a digitally deceptive environment. Benjamin (2024) introduces breaking information silos through a radical reframing of the current architecture of the web; with innovations such as the "Metaweb" or "Overweb", that provides "a decentralized public space above the webpage that enables the shift from personal to collective computing" (Bridgit DAO, 2023). While ElKattan (2024) advocates for the potential of cross-sector collaboration to "break down the barriers between academia, policy and public literacy" in order to better prepare digital users to navigate this ever-evolving landscape more safely.

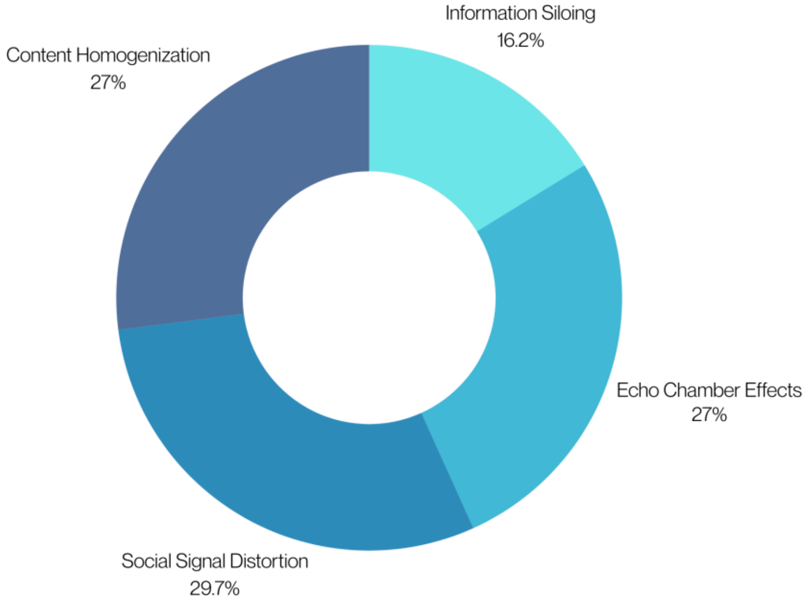
This necessity for an evolution of these critical evaluation skills is seemingly driven by what experts identify as the *complexity of verification* in the current age of digital deception. Harris (2024) frames this as an ongoing arms race: "There's an arms race between, say, the people who are trying to detect deep-fakes and the people who are trying to generate more and more lifelike deep fakes." Appleton (2024) takes this further, suggesting that verification complexity in digital spaces creates a "reality verification challenge", that through manipulation of content and social cues, threatens, not only our understanding of what is real online, but even our shared understanding of reality offline.

6.3. Knowledge Acquisition

Throughout the analysis, experts emphasized the growing difficulty of discovering, internalizing, and validating information within bot-dominated digital environments, highlighting how these challenges increasingly disrupt knowledge processes, signalling the reverberating effects on individual cognitive agency.

Figure 15

Knowledge Acquisition Distribution Chart



Note: Distribution of expert codes within the domain of Knowledge Acquisition, including *Information Siloing, Content Homogenization, Echo Chamber Effects* and *Social Signal Distortion.*

Information siloing represents a critical concern across multiple experts. Benjamin (2024) emphasizes how the current architecture of the web creates isolated knowledge environments through what they call “knowledge silos,” emphasizing the effect of algorithmic curation, echo-chambers and a limited web interface without implementations such as an Overweb; which aims to build a layer on top of the web that supports bridging information to create collective intelligence (Bridgit DAO, 2023). Schroeder (2025) describes a more extreme vision of what they term the “Antinet”, a web where “you cannot trust anything that you see online, and because everything is online... there is literally no information that if not spoken to you face to face by another human being, can be trusted”. Effectively jeopardizing the web as we know it, and how we may access digital information and communications in the future.

The experts also further identified concerning echo chamber effects, where synthetic content amplifies existing belief systems. ElKattan (2024) warns that bot-generated content creates "a problem of people caught in agreeability bias with bots, where it tends to give you answers that you want to hear," potentially creating echo chambers that they believe are worse than interacting with solely human users online. Appleton (2024) furthers how this bot interference impedes on knowledge acquisition, by illustrating how the introduction of hundreds of thousands of synthetic users, create manufactured social signals that make certain viewpoints appear more widely held than they actually are. 'Social signals' in this sense can be defined both technologically as the metrics associated with posts such as likes, shares, traction, that algorithms push due to perceived popularity (MailChimp, 2023) but can also extend to sociology as communicative or informative signals that directly or indirectly provide meaning (Poggi & D'Errico, 2011).

This manipulation of social signals poses perhaps the most significant threat to knowledge acquisition. As Appleton explains, "The median person does not have the skills or time or energy to seek out if something's bullshit or not online. So social signals are the proxy instead" (2024). When these signals are systematically manipulated, they fundamentally undermine how humans determine truth through social validation.

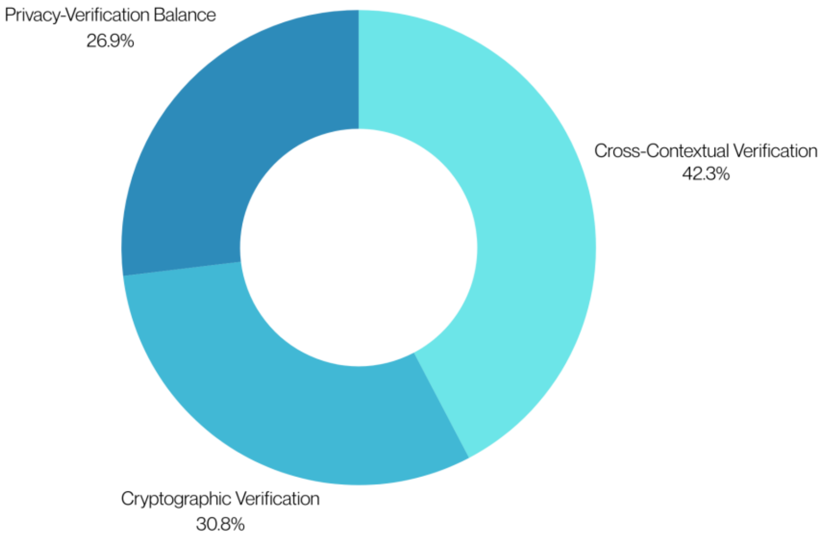
These challenges directly impact what Matta (2024) refers to as "cognitive liberty": the freedom to control one's own thinking processes. As personalized algorithms narrow information exposure and synthetic content floods these spaces, individuals experience diminished agency in knowledge exploration. This creates what Matta (2024) describes as "deterministic thinking patterns" that act as a "brake on creativity and motivation," inhibiting the diverse thinking necessary for robust knowledge acquisition.

6.4. Verification Practices

As digital verification systems increasingly fail under sophisticated manipulation, experts detailed how this reshapes authenticity establishment both online and offline.

Figure 16

Verification Practices Distribution Chart



Note: Distribution of expert codes within the domain of Verification Practices, including emergent and adaptive verification solutions, as well as the tension present in robust authentication and privacy concerns.

A significant approach termed *cross-contextual verification*, one that deliberately integrates methods spanning both digital and physical domains, emerged throughout the interviews. This approach recognizes that different contexts require varying verification thresholds based on factors such as criticality, security needs, and potential risk. Rather than applying uniform standards across all interactions, cross-contextual approaches assess verification according to the environment and stakes involved, implementing methods such as physical verification for high-security contexts while utilizing lighter verification for lower-risk interactions. While this approach may seem redundant, as it reflects current day verification practices, it does highlight that no sole practice or piece of technology will necessarily be our saviour.

Physical verification approaches featured prominently in expert discussions. Peter (2024) outlined current standards of verification for financial institutions, where physical presence in settings like bank branches serves as a critical authentication component. For social contexts, Appleton (2024) described establishing a “ring of trust where meeting in physical space validates people,” alluding to the potential for verification tiers that scale with physical interaction.

Community-based verification networks were also discussed with the potential to offer a more decentralized approach. Expanding on the 'ring of trust' model, ElKattan (2024) emphasizes trusted social circles established in the real world, where personal vouching creates verification based on established interpersonal trust. This approach may be particularly valuable for community platforms and semi-private digital spaces.

Experts also identified technical approaches including *Provenance* (the origin and creation history of a piece of content) *systems*, particularly suited for content verification across multiple contexts. Benjamin (2024) envisions these systems creating transparent trails of content origin that establish clear connections between content and producer.

Experts also identified purely digital authentication approaches for contexts where physical verification is impractical. Schroeder (2025) mentions the potential for “quantum encryption” and “one-time pads” providing mathematical certainty for highly sensitive digital transactions, while Benjamin (2024) emphasizes “zero-knowledge proofs” for privacy sensitive contexts.

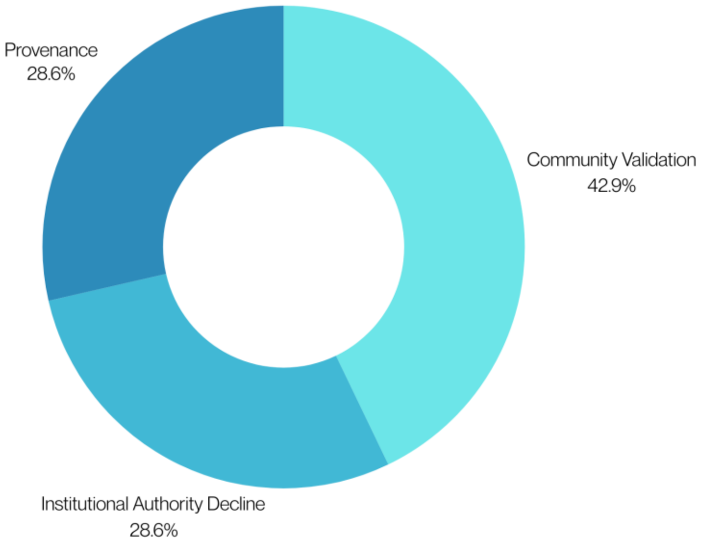
However, experts consistently highlighted a critical tension between *robust authentication* and *privacy protection* across these means of verification. ElKattan (2024) expresses caution about “overt authentication strategies that would require people's biometrics or state ID,” in the age of rampant data theft and institutional trust erosion, particularly for those whom anonymity serves legitimate purposes (such as activists, journalists & whistleblowers).

6.5. Credibility Assessment

Analysis of the expert interviews pointed to current and potential transformations in how credibility is established and evaluated in both digital and physical contexts. To recount, unlike verification practices that focus on confirming identity and authenticity, credibility assessment addresses the broader evaluation of information quality, reliability, and trustworthiness of the author or institution. Similarly, while trust formation examines the psychological and social dimensions of confidence development, credibility assessment focuses specifically on the processes of determining information believability.

Figure 17

Credibility Assessment Distribution Chart



Note: Distribution of expert codes within the domain of Credibility Assessment, with a majority of experts citing new and current means of community assessed credibility, methods of content provenance and the decline of institutions as credible authorities

Experts continuously noted the significant decline in institutions as an authority and marker of credibility. Important to note, this 'institutional authority decline' differs from the 'institutional trust transformation' discussed previously. While trust transformation addresses *the changing confidence in institutions* themselves, authority decline focuses specifically on *the reduced effectiveness of institutional endorsement as a credibility marker*. This reduced effectiveness is well described by DeIuliis:

> The field of communication has most often conceptualized gatekeeping as the selection of news, where a small number of news items pass a gate manned by journalists. In making their selections, gatekeepers construct social reality for the gated (Shoemaker, 1991). The World Wide Web has presented new challenges to these traditional models of gatekeeping, where raw content passes uni-directionally through a gate manned by journalists before reaching the reading public. The ability of users to create and disseminate their own content has uprooted and inverted the roles of gatekeeper and gated. (DeIuliis, 2015, p.1)

In the context of this broader shift in information dynamics, experts emphasized a growing concern over the erosion of credibility in online environments. Among a litany of possible causes for this decline, experts included the current proliferation of synthetic content across the web as a critical factor. As Lane (2024) illustrates "Even if you come across something that's genuinely reliable (online), you might still have concerns that it's not. Just the mere presence of misinformation can cause problems of your confidence in authentic information."

Several experts also noted that as public trust in large institutions (such as governments, corporations, and financial entities) declines, their authority as markers of credibility is increasingly called into question. Peter (2024), referencing the Edelman Trust Barometer from 2017, noted: "We're sort of on this edge of growing mistrust for large institutions: Government, large businesses, and so forth; and we have since that time moved very comfortably into mistrust." While they emphasized not having analyzed the banking sector specifically, they proposed that this broader decline in institutional trust *may be* shaping how people choose where to place their financial trust: "I think that this is influencing more specifically how people are choosing what institutions they bank with… That they *might* go to smaller institutions, rather or smaller businesses." (Peter, 2024). This observation also aligns with ongoing trends in public behavior and consumer sentiment. A *Wall Street Journal* report (Moise, 2024) documents consumers switching from major banks to community banks, and similarly, a *Time Magazine* feature notes that Millennials, shaped by economic instability and the fallout of the Great Recession, are "skeptical of anything they hear from a financial institution," with one-third reportedly ready to switch banks within 90 days (Kadlec, 2014). Taken together, these trends suggest a growing preference among some for smaller, more transparent, and tailored institutions; particularly when large institutional affiliation no longer functions as a reliable marker of credibility or public trust.

As institutions wane in their credibility, and the public looks to alternative sources or individuals, *provenance*, as previously discussed, emerges as a possible credibility marker, at least for online content. Benjamin (2024) emphasizes the importance of "understanding where content came from and who generated it (human or machine)" and advocates for systems that allow users to track content history and provenance. Rather than relying on an institutional checkmark, users are increasingly evaluating credibility through a process that examines a content's origins; however, this currently involves a set of evolving, and often inconvenient, digital literacy skills.

Community validation also emerges as a significant pattern in evolving credibility assessment. Community validation creates a distributed means of assessment that may prove more resilient to synthetic manipulation than a centralized authority. Harris (2024) notes "some promising research on crowd sourcing judgments of accuracy using basically the same principle as something like the community note features on Twitter," suggesting that "doing this via crowd sourcing you get a bit less worried about top-down control." Meanwhile, ElKattan (2024) describes the retreat to smaller networks of trusted members (i.e. Dark Forests) as a means of communally identified credible sources or actors.

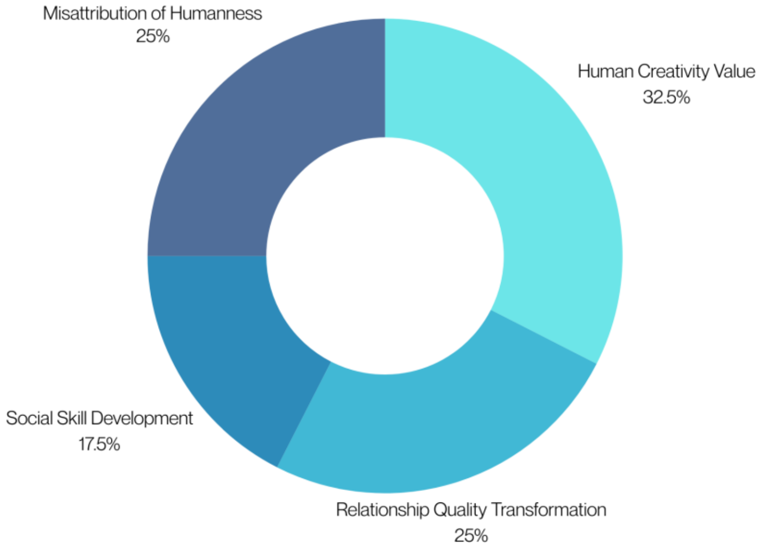
These emerging challenges concerning credibility systems acknowledges what Eysenbach (2008) identified as the contemporary challenge of the web: where individuals must evaluate vast amounts of online information on their own; increasingly within synthetic environments, while navigating growing skepticism toward both the sources and the actors they engage with.

6.6. Social Impact

Perhaps the most widely discussed set of challenges across the interviews concerned the current and potential transformations in human social dynamics as a result of this burgeoning dead internet and emerging technologies. Specifically, experts focused on how human interactions with synthetic entities and content reshape relationships, skill development, community formation, and even fundamental perceptions of humanity. They further that these changes extend beyond digital environments and significantly influence physical-world experiences and interpersonal connections.

Figure 18

Social Impact Distribution Chart



Note: Distribution of expert codes within the domain of *Social Impact*, including how human relationships, values and social skills are developing in the current a future digital age

One of the largest concerns identified by experts revolved around relationship quality transformation. Peter (2024) describes how technological dependence results in “behavioral alienation” and “thinning human relationships”, while Appleton (2024) furthers that relationship skills “are going to degrade if you're not engaging with actual humans and their weirdness, and quirks, and difficulties” illustrating how synthetic entities are altering human connection expectations.

This relationship transformation reflects what Turkle (2017) identifies as technology becoming the “architect of our intimacies,” reshaping how individuals relate even offline. Experts suggest that these interactions, whether by human-to-AI, or a curation of content, exacerbated by bot networks, leads to echo-chambers and may subtly alter expectations of relationships by removing the friction of a diversity of thought (fundamental aspects of humans and their relationships). As ElKattan (2024) notes, there's “always a ceiling to how a connection can go” with a bot, yet their *predictability* and *accommodation* may create preference for low-conflict relationships or interactions that fail to develop fundamental social skills.

The implications for social skill development emerges as a particularly concerning dimension, especially for younger generations. Beasy (2025), specifically describes a silver spoon effect where children interacting primarily with accommodating bots develop “shortened attention span/patience and unwillingness to engage in human messiness due to the speed of automation.” This implication reinforces Gunadi, & Lubis’s (2023) previously discussed study, detailing the severe developmental problems posed to children due poor digital literacy skills (Gunadi, & Lubis, 2023).

Simultaneously, experts identified the evolving nature of community formation in response to these social skill and relationship quality declines. ElKattan (2024) illustrates the retreat from public channels and fragmentation of digital communities; a shift that may unintentionally deepen echo chambers rather than dissolve them. Harris (2024) warns specifically about these feedback loops, wherein synthetic content and algorithmically curated feeds amplify existing beliefs. These algorithmically reinforced communities diminish exposure to diverse perspectives and nuanced discourse, eroding the social skills needed for navigating differences, revealing the tension between echo chambers in public and private channels alike.

The consequences of these digital patterns are seemingly affecting the formation of *physical* communities as well. Appleton (2024) describes how synthetic content manipulates apparent consensus through “hundreds of thousands of synthetic users” creating false social signals. As such, this drives users to connect with those offline who also align with these artificially amplified beliefs. Conversely, echo chambers and algorithmically curated communities, as stated previously, may impede on community formation, as individuals seek relationships in their community that increasingly only align with *their* views.

Experts also point to the ‘misattribution of humanness’, namely for interactive technologies such as generative AI or synthetic actors, as harmful to social development. ElKattan (2024) asserts that “people thinking they're speaking to a human when they're not is unethical,” and Peter (2024) warns of humanizing of non-human actors where, “once you build trust and dependence and reliability in a software program, that is misplaced.” Appleton (2024) furthers the deception involved in this relationship stating: “there's not actually a human there that I can have a real relationship with. There's not someone who can actually come help me in a time of need.” Sherry Turkle (NPR, 2024) recently expanded on this notion, warning that the rise of this “artificial intimacy” reflects a troubling shift in human relationships, as people increasingly seek out connections devoid of vulnerability, forgetting, as she puts it, that “vulnerability is really where empathy is born,” and that machines merely exhibit “pretend empathy” rather than genuine care.

However, personal AI assistants represent a potential counterbalance to these challenges. Benjamin (2024) describes “AI tools using private data vaults to improve personal decision-making” that could enhance rather than replace human capabilities; noting access to health data possibly improving diet and exercise recommendations, or access to communications channels may enhance one’s organization capabilities. Peter (2024) notes the potential dual nature of these human-AI relationships, suggesting “on the positive side, it's that collaboration that enriches and extends both. It enriches and extends the human. Because you now have this generative partner.”

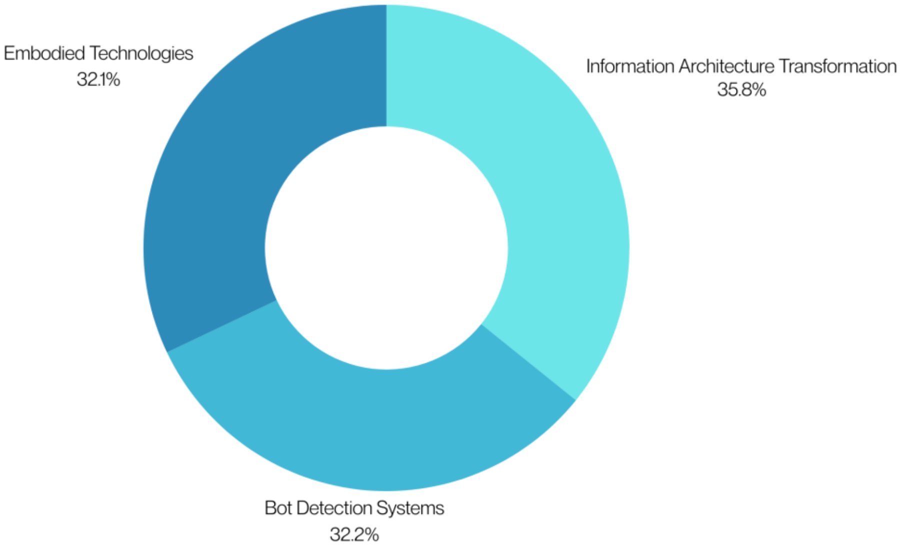
Personal AI assistants were noted throughout the interviews for both their present potential benefits, but also for their potential future concern. Peter (2024) warns about dependency issues where “we're just becoming more and more addicted to the machines,” creating what Schroeder (2025) describes as a “loss of the private personal experience of the world” where “our entire experience to the world becomes mediated.” This “mediation” potentially obfuscates our sense of reality through what ElKattan (2024) calls “agreeability bias” where AI systems “give you answers that you want to hear”, potentially even mediating frictive communiques to your so-called ‘benefit’. Peter (2024) further notes how “convenience trump's privacy” in these relationships, raising significant data privacy concerns, as personal assistants require extensive access to private information.

6.7. Tools & Technologies:

The following chapter illustrates the technological developments shaping user experiences in increasingly bot-dominated digital environments. These tools represent both the systems enabling synthetic activity and the countermeasures deployed to identify and mitigate it.

Figure 19

Tools & Technologies Distribution Chart



Note: Distribution of expert codes within the domain of Tools & Technologies, including evolving bot detection systems, the infiltration of embodied technologies and potentials for restructuring the information architecture of the current web.

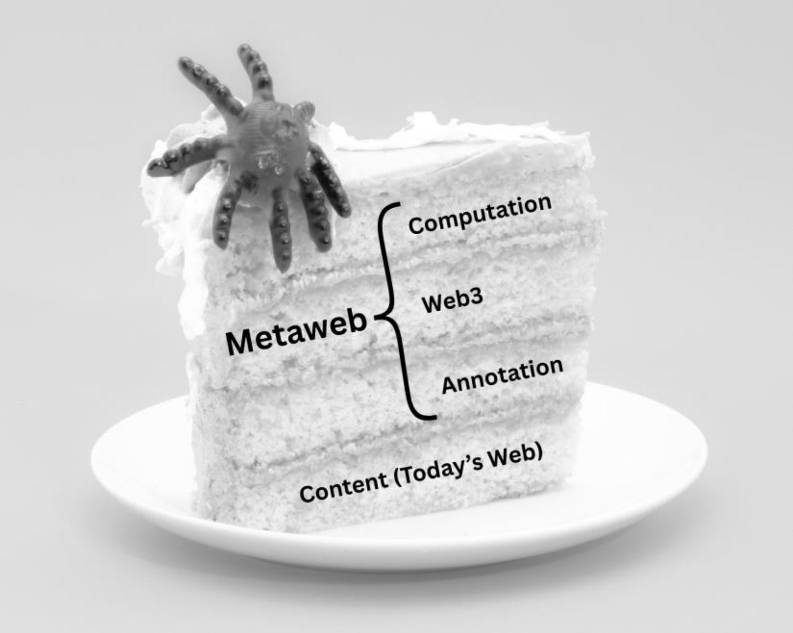
One of the most radical transformations that was discussed regarded a fundamental transformation of the current architecture of the web in response to synthetic activity and content. Benjamin (2024) references a new model of the current web altogether with the introduction of the Metaweb. The Metaweb proposes: “A Decentralized public space above the webpage that enables the shift from personal to collective computing… a hyper-dimensional web over Today's Web that connects people and information silos, with accountability and fair value exchange” (p.i). The Metaweb also proclaims it can:

> Drastically reduce false information, abuse, and scams, as well as enable the unprecedented level of collaboration needed to address humanity’s global challenges. The book posits a symbiotic relationship between AI and the Metaweb, where AI assists in generating, organizing, and curating content, while the Metaweb provides the necessary data and context for AI to function effectively, transparently, and in alignment with humanity. The AI-assisted collaboration among humans on the Metaweb will enable a vast collective intelligence. (Bridgit DAO, 2023, p.i)

In order to better visualize this proposed public space above the webpage, Brigit DAO (2023) provides the visualization of a “four-layered web cake” model adapted in **Figure 20**.

Figure 20

The Four-Layer Web Cake



Note: An adaptation of the visualization of the four-layered web model. The base layer represents Today's Web (static content), while the Metaweb comprises three emergent layers: Annotation, Web3 functionality, and Computation. Each aims to enable greater interactivity, decentralization, and agency in digital environments. Adapted from *The Metaweb: The Next Level of the Internet* (1st ed., p. 4), by Bridgit DAO, 2023, CRC Press. https://doi.org/10.1201/9781003225102. Copyright 2023 by CRC Press. Used under fair dealing for research and educational purposes.

The "four-layered cake" model offers a restructuring of the current web architecture, envisioning an internet that extends beyond flat, static content into a multi-dimensional, interactive system (Bridgit DAO, 2023). In this model, "Today's Web" forms the foundational layer, while the Metaweb introduces successive layers of annotation, decentralized functionality (Web3), and programmable computation (Bridgit DAO, 2023). Together, these layers reconfigure the web from a passive interface into an active, user-driven environment (Bridgit DAO, 2023).

This radical proposal comes on the heels of the plethora of challenges that plague Web1.0- 3.0 expressed throughout this research, but Bridgit DAO specifically notes how:

> Bots play a significant role in amplifying and proliferating artificial trends. Bots drive the conversation because they are lightning fast, controllable, and don't need breaks. Web users must copy the bots to stay on-trend. Bots are an indispensable tool for manipulation, because they will not go off-script. We don't subscribe to the theory that AI generates most online content. But it may soon…A large-scale experiment proved that nobody—neither Twitter admins, tech-savvy social media users, nor innovative applications—can distinguish bots from legitimate users… the Web is full of duplicative, artificial, and fake content. (Bridgit DAO, 2023, p.106)

Furthering this notion of a radical transformation of the web, Schroeder (2025) describes the potential for the current internet to evolve into what they term the “Antinet”, an internet that is overtaken by bots and effectively ‘dead’ and furthermore, unreliable.

However, the progression of bot detection systems represents another potential technological response. Benjamin (2024) describes the potential for “bot versus bot” applications where specialized AI systems identify synthetic content; Lane (2024) emphasizes watermarking approaches, similar to provenance approaches, while Appleton (2024) predicts entire “truth verification industry” careers (similar to digital private investigators). However, these systems face sophisticated countermeasures including IP cycling, proxy networks, and CAPTCHA circumvention techniques (Imperva, 2024a; Searles et al., 2023, p.10) that threaten to outpace defensive measures.

Perhaps most concerning, looking toward potential futures, is the expansion of technology from digital spaces into the fabric of physical life. This shift includes wearable technologies, but more profoundly signals a trajectory of digital systems becoming embedded within the human body, cognition, and self-perception (Nelson et al., 2019) also known as “embodied technologies”. Schroeder (2025), warns of the internet no longer being considered a separate medium, but to one where intelligence is being built “into every object that we manufacture.” They further that this evolution presents two competing economic models: one where “everything is owned by a tiny elite and the rest of us merely rent it,” exemplified by John Deere tractors and Tesla vehicles (where manufacturers maintain ownership through embedded software) (Wiens, 2015; Perzanowski, 2016); and another where “every object owns itself and communicates with other objects and with people” (Schroeder, 2025) to optimize usage. Both models fundamentally “move the Internet out of the cloud and into your house. And onto your wrist and into your pocket,” creating environments where “bots can be literally anything, anywhere” (Schroeder, 2025). This transformation dissolves the boundaries between digital and physical realms, leaving individuals surrounded at all times by what Schroeder terms “a cloud of lying demons” potentially present in “your phone, your TV, your landline” (2025).

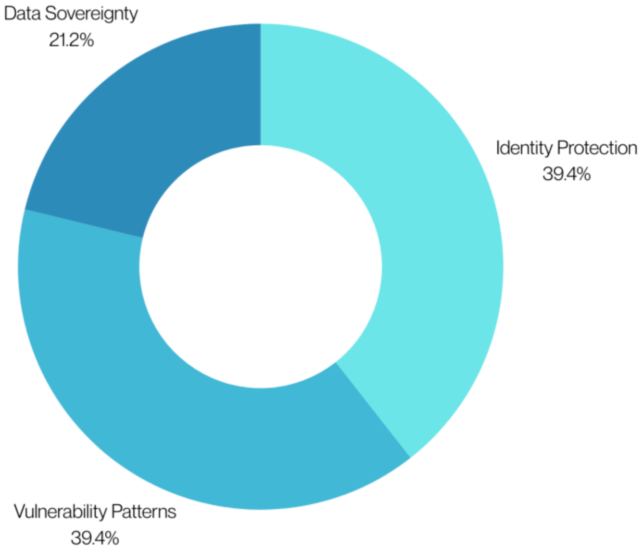
Lane (2024) emphasizes these vulnerabilities but extends them from personal items to current critical infrastructures. They contend that critical infrastructures such as water supply systems are directly connected into the Internet and that the potential for digital attacks, as already evidenced by a slew of recent, high-profile breaches in water systems (Rosenbaum, 2024), may result in catastrophic physical consequences.

6.8. Privacy & Security Systems

Privacy and security challenges reoccurred throughout the analysis, considering how synthetic technologies reshape current systems and digital environments.

Figure 21

Privacy & Security Systems Distribution Chart



Note: Distribution of expert codes within the domain of Privacy & Security Systems including *Identity Protection, Vulnerability Patterns* and *Data Sovereignty.*

Identity protection consistently emerged as a critical concern as synthetic technologies are able to more effectively impersonate human activity. Beasy (2025) emphasizes deepfake security threats requiring new verification mechanisms, while Appleton (2024) specifically warns about voice cloning where attackers "can just call you and pretend to be one of your relatives" and Schroeder (2025) describes sophisticated "video fraud threat" scenarios where deepfakes enable business scams. Seemingly, these technologies are currently able to spoof three of our five senses, and these threats extend beyond deception of laypeople, as evidenced by the cybersecurity firm KnowBe4 hiring a North Korean hacker using AI-assisted deepfake videos to create a false identity (Sjouwerman, 2024).

Developing data sovereignty systems also offer potential solutions to privacy concerns. Benjamin (2024) proposes "communities owning and monetizing their data through cooperatives" alongside "AI tools using private data vaults to improve personal decision-making." These sovereignty approaches attempt to balance verification needs with privacy protection while also rebalancing data-power relationships. They enable what Benjamin (2024) describes as "decentralized ownership of data" where individuals and communities maintain control over their information while potentially monetizing it themselves, a departure from the current model of data extraction.

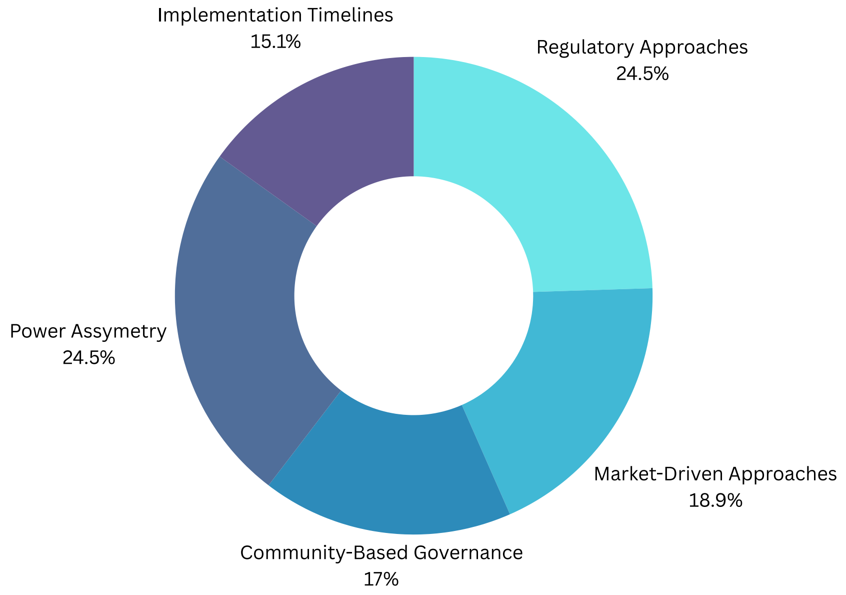
The risks posed by privacy failures on vulnerable populations were also highlighted by experts. Peter (2024) identifies specific vulnerable groups including "senior citizens, newcomers, and those less digitally savvy" facing disproportionate exploitation risks as bot technologies become more sophisticated. ElKattan (2024) emphasizes how these technologies affect "those who are most vulnerable," while Appleton (2024) describes digital security as "playing Russian roulette" where "none of us are safe." These vulnerability patterns ultimately create what Peter (2024) characterizes as an increasing financial inequity. They contend that access to these technologies further "alienate and contribute to the disparity" between those with technical capabilities and those without.

6.9. Governance & Policy

The expert analysis reveals the complexity of governance challenges in regulating increasingly sophisticated synthetic entities, content and those who deploy them. These challenges extend to jurisdictional boundaries, policy lag, market dynamics, growing asymmetries of power, and even fundamental ideological tensions concerning the governance of the web.

Figure 22

Governance & Policy Distribution Chart



Note: Distribution of expert codes within the domain of Governance & Policy including varying approaches to current and future governance, growing power asymmetries with relationship to compute and access, and the timelines necessary in order to enact policies.

The expert interviews identified a diversity in regulatory approaches. Beasy (2025), emphasized the limitations of AI regulation across jurisdictions, noting that "laws and regulations will only do so much... so long as there's plenty of AI models that are open source" noting how access to these technologies has grown so significantly in recent years. Lane (2024) predicts regulation will only come on the heels of a crisis: "Something will happen... and legislators will move very, very fast", alluding to a *reactionary*, rather than a *proactive* approach to regulation, often coming too late to prevent significant harm. Simultaneously, ElKattan (2024) highlights the need for "government regulation for government actors" as equally important, considering state entities themselves deploy synthetic entities for public manipulation, such as Russia's *Internet Research Agency* interference in the 2016 U.S. Election (Lukito, 2020).

Alternatively, market-driven solutions also emerged during the interviews as a governance mechanism, though with significant limitations. Harris (2024) anticipates that platforms and systems may change to accommodate users' needs, suggesting that for example "a platform that has better anti-bot policies would become, overtime, more popular" than those with weaker protections. However, Lane (2024) presented a more fatalistic market view, predicting that users will abandon services only after some significant harm is identified, suggesting market corrections may occur, but only after it's too late.

Community-based governance offers a third approach identified in our research. Benjamin (2024) emphasized community data cooperatives and collective standards development, while ElKattan (2024) advocated for multi-pronged approaches in order "to break down the barriers between academia, policy and public literacy." Harris (2024) focused on "crowd-sourcing judgments" without "top down control," linking to the possibility of distributed governance models that attempt to overtake traditional regulatory bottlenecks.

However, internet governance faces fundamental challenges. Beasy (2025), highlighted the jurisdictional challenges involved, illustrating how "foreign actors... not subject to the same laws" limit regulatory effectiveness, while ElKattan (2024) emphasized how state actors "flood social media with certain rhetoric" for political influence across borders. Ideological tensions further complicate the ability for internet governance as Schroeder (2025) describes the potential for techno-oligarchic control creating a "permanent state of inequality and oppression," while ElKattan (2024) emphasized "power asymmetry in technological access" where only "actors that have the financial capacity, the power, and the dedication" can effectively deploy sophisticated synthetic technologies. Appleton (2024) reinforced this concern, warning how "money essentially amasses to people who have access to compute."

Lastly, implementation timelines by governmental bodies also present additional challenges. Lane (2024) identified a 30–40-year cycle from technological implementation to regulatory remediation, noting that remediation typically requires "30 years minimum" because "it usually takes five to 10 years to even get a public inquiry. And then that takes another 10 years." This creates extended periods of vulnerability with potentially significant social costs.

6.10. Concluding Remarks on Findings

The findings across the neo-ecological domains reveal a rapidly evolving sociotechnical landscape marked by disruption and deepening complexity. If the experts are correct, *trust*, once anchored in recognizable social cues and institutional authorities, is now caught in recursive cycles of collapse and renewal, as technological verification struggles to keep pace with increasingly sophisticated synthetic actors. Yet this arms race does not occur in a vacuum, it is actively reshaping the very processes through which trust is formed and sustained in both digital and physical environments.

Digital literacy is now being outpaced by the demands of an environment shaped by a rapidly evolving technological environment that laypersons struggle to keep apace with. Experts repeatedly emphasized the need for new tools to navigate this increasingly unsafe and dying web. Tools that include, not just the capacity to evaluate information, but to navigate a world where even basic signals of authenticity are easily forged. This connects directly to challenges revealed in *Knowledge Acquisition*, where siloed environments, echo chambers, and social signal distortions actively undermine users' ability to access diverse or trustworthy information.

Across the interviews, experts noted the ironic return to physical forms of authentication as digital mechanisms fail, alongside the push for more community-based mechanisms and the advent of provenance tracking in order to create content trails. Yet, these systems bring their own tensions, particularly in balancing verification with privacy and autonomy, as well as the burden of verification placed on the user.

The decline of institutions as a credible authority marks another critical shift. Experts once again pointed to the emergence of community-based validation as a response to the unreliability of traditional endorsements, pointing to credibility as something increasingly socially negotiated. However, this shift also comes at a time of increased vulnerability to digital manipulation, particularly as synthetic actors fabricate signals of consensus.

Perhaps most significantly, the social impact of these transformations reflects deeper questions about what it means to be human in digital environments. The degradation of social skills, the misattribution of humanness, and the reshaping of relationship norms through interactions with synthetic entities underscore not just *behavioral* changes, but *existential* ones. The domain of *Tools & Technologies* highlights how embodied technologies increasingly determine what users see, believe, and do, while *Privacy & Security Systems* may continue to struggle to contain or manage these forces.

Finally, the *Governance & Policy* domain revealed tensions between jurisdictional reach, market self-governance and growing sovereign intranets ceding from the public square. Regulatory systems appear reactive, latent and fragmented, with global coordination remaining seemingly impossible as power asymmetries grow for those with compute power, access and control (setting the stage for techno-oligarchism to thrive).

Together, these insights surface a set of interconnected challenges that extend beyond traditional technical problems. They point to an epistemic transformation. A shift in how individuals determine *what is real*, *who is credible*, and *what can be trusted*. These dilemmas are not easily resolved by any single policy or product. They are systemic and existential in nature.

As such, the foresight inquiry that follows builds directly on these findings, not to offer a prediction, but to explore how these tensions might unfold, intersect and/or intensify over time. By constructing plausible futures and identifying critical uncertainties, the scenarios that follow allow us to surface additional insights, and design more considered interventions.

7. Foresight: *Worlds in the Making*

Building on the preceding SotA review, expert interviews and RTA, this chapter extends our inquiry utilizing strategic foresight methods. While the expert insights revealed the current and potential dynamics of synthetic content and bot proliferation, foresight allows us to examine how these trends may evolve and interact in the coming 5 to 10 years in order to better ascertain recommendations across estimated timelines and actors.

The foresight process employed here is not about predicting a singular outcome, but about exploring plausible futures. It allows us to imagine how emerging disruptions, such as the 'breakdown of digital trust' or 'the lack of sufficient technological oversight', might develop across domains and influence various facets of the human experience. As such, foresight serves as both an *extension* and a *lens* through which to recontextualize the research findings and consider *this is where we could go next.*

Informed by recurring and meaningful insights ascertained throughout this research study and organized through the STEEP+V framework (Social, Technological, Economic, Environmental, Political, and Values), the ten change drivers introduced in the following section highlight major systemic shifts with the potential to shape a future increasingly mediated by synthetic entities, content and emerging technologies. These drivers offer the foundation for the scenario development that follows, where critical uncertainties are mapped across a 2x2 matrix to explore four, distinct, plausible futures.

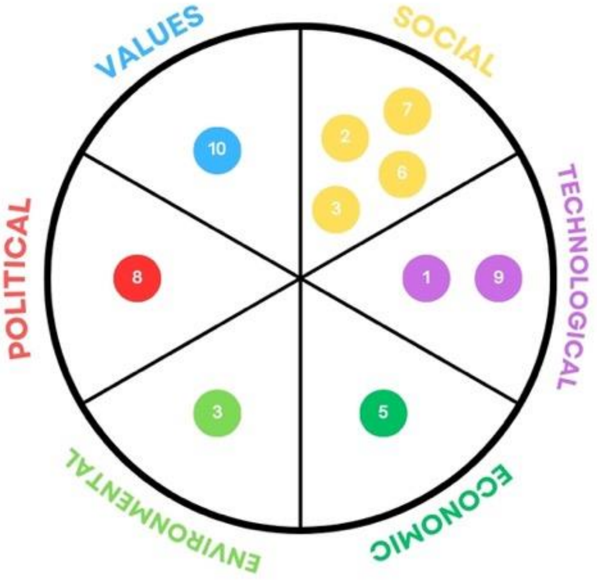
7.1. Change Drivers

To better understand the systemic impacts of bot proliferation and synthetic content, this chapter identifies ten major drivers of change. In doing so, it briefly shifts from the neo-ecological framework to the STEEP+V framework (Social, Technological, Economic, Environmental, Political, and Values), which offers a broader lens for spotting and organizing drivers of large-scale transformation.

Policy Horizons, the foresight arm of the National Government of Canada, defines change drivers as large developments with the potential to significantly disrupt one or more elements of a system (Policy Horizons, 2024). Organizing these drivers through STEEP+V, as exemplified in **Figure 24,** aims for a well-rounded scan of external influences buoyed by this research study, setting the stage for scenario development and the exploration of future possibilities.

Figure 23

STEEP+V Organization of Change Drivers



Note: This figure illustrates how each of the ten change drivers aligns with the STEEP+V framework. The numbers within each segment correspond to specific change drivers, indicating which drivers are most closely associated with each category.

Rather than treating the future as a single trajectory, these drivers reflect a set of interacting forces reshaping how humans verify truth, form relationships, and construct both shared and personal realities. Each driver highlights a disruptive tension or transformation already underway, offering a foundation for the scenarios that follow.

For further details as to how change drivers were analyzed and categorized, please refer to ***Appendix E***

7.1.1. The Significant Drivers of Change

1. *Technological Verification Arms Race:* The escalating technological battle between *verification systems* and *deception technologies*. As synthetic entities become increasingly indistinguishable from authentic users, traditional verification mechanisms are failing, while new systems struggle to keep pace with technological advancements. This creates cycles of innovation followed by circumvention, with deepening impacts on the foundation of trust online. **Level Impact:** Microsystem (individual users encountering synthetic content), Exosystem (technology developers and cybersecurity firms creating verification tools)

2. *Trust Splitting:* Rather than simple erosion, trust is evolving into two extremes: *hyper-skepticism toward legitimate and institutional sources*, alongside *misplaced overconfidence in certain synthetic or alternative sources*. This "trust split" reshapes our pattern of information evaluation and subsequently relationship formation, based on lack of a "shared reality". **Level**

Impact: Microsystem (individuals forming personal trust judgments), Mesosystem (interactions between individuals and their immediate social groups)

3. ***Physical-Digital Boundary Break:*** The expansion of technologies from digital spaces into physical environments through IoT, embodied AI, and smart infrastructures creates new vulnerabilities. This driver transforms *everyday objects* into *potential synthetic agents*, and the escalation of digital wearables blurs the line between virtual and physical experiences; threatening the last vestige of unmediated reality: our physical perception. **Level Impact:** Microsystem (individuals interacting with smart devices in daily life), Mesosystem (integration of technology in homes and workplaces), Exosystem (manufacturers of IoT and AI embedded technologies)

4. ***Social Signal Manipulations:*** The deliberate distortion of social cues online that humans use for truth determination (such as making certain viewpoints appear more widely held than they actually are online) are undermining epistemological processes and transforming the mechanisms humans have evolved to rely upon in order to determine *consensus* and *truth*. **Level Impact:** Microsystem (users interpreting social cues online), Mesosystem (communities and peer groups), Exosystem (social media platforms and content algorithms)

5. ***Data Sovereignty Movement*****:** The emergence of novel data ownership models challenges the current extraction-based model. This represents a powerful driver as the potential for communities to own and monetize their data through cooperatives, alongside access to personal data vaults, restructuring power relationships in digital environments. **Level Impact:** Exosystem (organizations managing data ownership and privacy tools), Macrosystem (national and international policies on data rights)

6. ***Retreating to the Dark Forests:*** The escalating withdrawal of users into verification-based communities, such as Discord or WhatsApp groups, as a response to the current state of public platforms, also represents another powerful driver. These Dark Forests (Strickler 2019; Appleton, 2023) may evolve to swaths of users on the web relying on private digital spaces with personally vetted sources in order to form a sense of trust and authentication. **Level Impact:** Microsystem (individuals seeking private and/or trusted online spaces), Mesosystem (closed online groups and public internet communities)

7. ***Relationship Quality Transformation*****:** The alteration of human connection expectations due to interactions with synthetic entities represents a large social driver. As humans increasingly engage with synthetic entities, our relationship skills risk atrophy. We lose the essential practice of navigating the messy terrain of human connection with its weirdness, quirks, and difficulties that make authentic relationships both challenging and meaningful. This substitution leaves us ill-equipped for the beautiful complexity of genuine human bonds, suggesting large impacts on social development that affect our means of interpersonal connection. **Level Impact:** Microsystem (personal interactions with synthetic entities), Mesosystem (family and social relationships influenced by technology use).

8. ***Webs with Borders:*** The increasing inability of internet governance to be enforced by national regulatory bodies creates ongoing difficulties to the challenges posed by bots and the actors that deploy them. As Post and Johnson (1996) note, digital environments "disregard geographical boundaries" and "cannot be governed satisfactorily by any current territorially-based sovereign" (p. 1375). This creates fundamental tensions as countries such as Russia and China advocate for state-controlled internet systems, while Western democracies pursue different regulatory approaches, such as the Canadian Government banning access to news content on Facebook and Instagram (Mundie, 2023). **Level Impact:** Macrosystem (government policies and international agreements on internet governance)

9. *Web 4.0, 5.0, 6.0… :* The escalating strain on the current web structure from synthetic activity creates pressure for fundamental redesigns. Advents to these structures and systems, such as the "Metaweb", may offer novel solutions like a decentralized public space above the webpage that enables the shift from personal to collective computing. This architectural pressure could reshape how humans interact with the web moving forward. **Level Impact:** Exosystem (developers and organizations designing next-generation web architectures)

10. *Reality Construction:* This *meta-driver* represents the culmination of many significant drivers, pointing to the systematic manipulation of mechanisms that humans use to establish and maintain reality. From challenges to cognitive liberty, to social verification, to sensory perception, this driver escalates the concern of digital manipulation, to questions about how we preserve both individual and shared reality when the processes for establishing what is real becomes increasingly vulnerable to technological influence. **Level Impact:** All Levels (Microsystem: individual perception and cognition; Mesosystem: social interactions shaping shared realities; Exosystem: technology influencing information environments; Macrosystem: governing bodies and cultural norms influencing reality constructs)

The drivers above illustrate the complex transformations at hand, that extend beyond just the technical challenges of content authenticity online. They point to the undergoing shifts in how humans *establish trust*, *form relationships*, *acquire knowledge*, and even *construct their realities*. What emerges is not simply a story of technological evolution, but a reconfiguration of the mechanisms by which we understand and navigate both digital and physical worlds.

Particularly significant is the potential for these drivers to interact with each other as they develop alongside each other, rather than in silos. Such interactions create the foundation for our scenario development, examined in the following chapter.

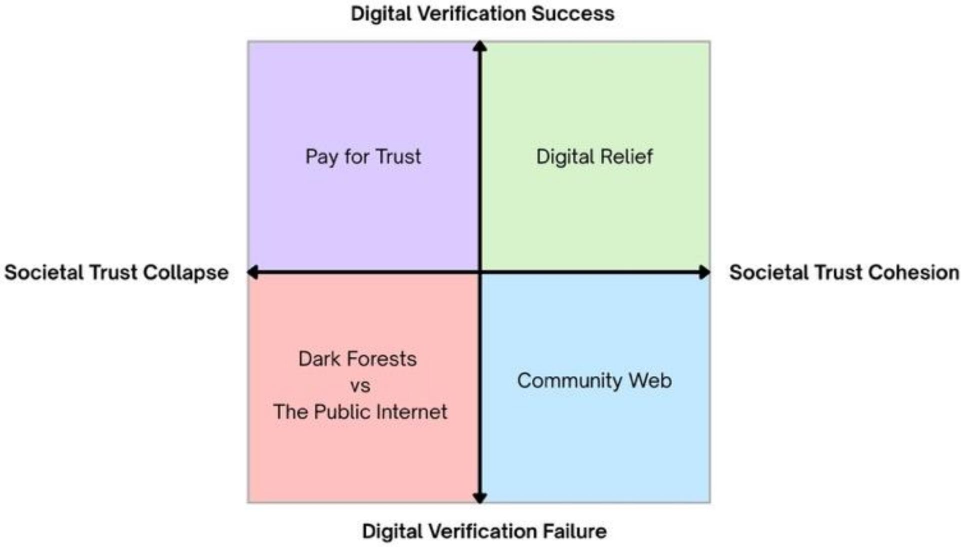
7.2. Scenarios: *The Futures Between Collapse and Cohesion*

In this chapter, we explore four distinct potential futures based on critical uncertainties utilizing the 2x2 Scenario generation technique (Schwartz, 1996, pp. 241-248). These scenarios help to illustrate and prepare for the range of ways bot proliferation may reshape human experiences.

After careful consideration of coverage, relevance to the research question, and narrative potential, "Digital Verification Capability" (Success vs. Failure) and "Societal Trust Patterns" (Collapse vs. Cohesion) were selected as the critical uncertainties with greatest potential for generating meaningful contrasts.

Figure 24

2x2 Matrix of Digital Verification Capability & Societal Trust Patterns



Note: This 2x2 matrix maps four plausible future scenarios based on the intersection of two critical uncertainties: Digital Verification Capability (Success vs. Failure) and Societal Trust Patterns (Collapse vs. Cohesion). Each quadrant represents a distinct future world shaped by different combinations of these uncertainties.

The intersection of these uncertainties created four distinct scenario quadrants, each representing a plausible future world:

- ***Pay for Trust*** (Digital Verification Success × Societal Trust Collapse): Reflecting a world where verification becomes a commercial service creating new forms of inequality.
- ***Digital Relief*** (Digital Verification Success × Societal Trust Cohesion): Depicting a world where verification technologies outpace offensive strategies and support a renewed sense of social cohesion.

- ***Dark Forests vs. Public Internet*** (Digital Verification Failure × Societal Trust Collapse): Illustrating a split digital landscape where trusted spaces become increasingly exclusive while the public internet continues to run wild.
- ***Community Web*** (Digital Verification Failure × Societal Trust Cohesion): Portrays a world where community-based approaches attempt to compensate for technological limitations, even as bot technologies grow.

These naming choices deliberately avoided simplified language such as "utopia" or "dystopia," instead focusing on the nuance of each potential future within the 5-10 year frame, recognizing as well that each scenario presents both opportunities and challenges for different stakeholders.

7.2.1. A Brief Snapshot

To contextualize the scenarios that follow, the table below offers a comparative overview of how the challenge domains shift across the four imagined futures. It distills insights from each world and highlights how specific challenge domains manifest under different conditions.

This framework loosely adapts Dator's Four Generic Futures (Growth, Collapse, Discipline, Transformation) into a matrix to suit the aims of this research. While Dator's model sketches broad societal trajectories, this matrix narrows its focus to the defined challenge domains explored throughout the study. The table serves as both a point of comparison and an entry point into the full scenario narratives that follow.

Table 5

Comparative Matrix of the Four Worlds

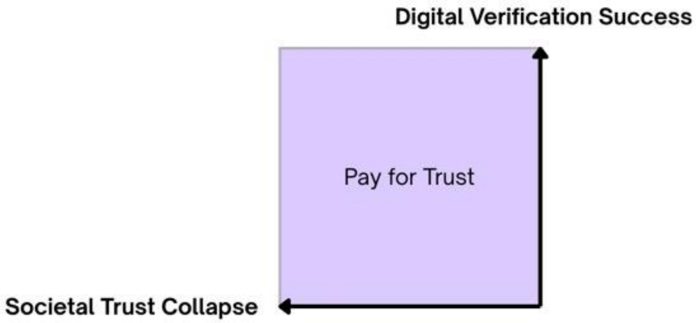
Domain	Pay for Trust	Digital Relief	Dark Forests vs. Public Internet	Community Web
Trust Formation	Monetized	Collaborative	Fragmented	Community-driven
Digital Literacy	Survivalist	Foundational	Unequal	Participatory
Knowledge Acquisition	Gated	Transparent	Segregated	Pluralistic
Verification Practices	Tiered	Contextual	Socially mediated	Distributed
Credibility Assessment	Proprietary	Multi-layered	Community-biased	Layered
Social Impact	Hierarchical	Cohesive	Polarized	Reconnected

Tools and Technologies	Proprietary	Open source	Fragmented	Decentralized
Privacy & Security Systems	Trade-off	Balanced	Compromised	Privacy-preserving
Governance & Policy	Captured	Coordinated	Fractured	Contested

Note: This matrix contextualizes each of the domains across the four future scenarios to more clearly convey the nature of each world and highlight their key divergences.

7.2.2. Scenario 1: Pay for Trust

(Digital Verification Success × Societal Trust Collapse)



By 2035, verification technologies have solved the *technical* challenge of detecting synthetic content but created perhaps something worse... a society where safety and trust online have become *luxury products* available primarily to those who can afford them.

Trust Formation hasn't *democratized*, it's been *monetized*. What began as "premium features" on social platforms has evolved into digital trust ecosystems where verification access directly correlates with the size of your wallet. Premium users have exceedingly more confidence in digital information through sophisticated verification systems that authenticate content and users, while those with basic access navigate environments of perpetual uncertainty *(**Driver: Technological Verification Arms Race**, verification outpaces access and creates new inequalities).*

This trust has extended into the physical realm, where premium users function as modern knowledge barons. These digital aristocrats wield decisive information that ends debates and shapes perceptions of reality itself. Their peers instinctively defer to them to determine what is true. We have regressed to hierarchical knowledge relationships reminiscent of earlier eras, where trust is built not on democratic access to information but on privilege and exclusive technological access *(**Driver: Reality Construction**, regress to epistemic).*

Verification Practices have flourished as a thriving market, with tiered packages becoming the industry standard. Major platforms offer multi-level trust subscriptions: "Basic" (minimal verification with some exposure to synthetic content), "Standard" (personal verification with stronger content verification), and "Premium" (comprehensive verification with AI watermarking and reliability mechanisms). Those with premium packages live in digital environments where content and users undergo sophisticated authentication, while the rest continue to struggle to tell human from bot, fact from fiction, and increasingly abandon the web as a resource *(**Driver: Web 4.0, 5.0, 6.0...**, desire for new construction of the web has increased by those less fortunate but requires capital only held by those who don't see a problem with the current web).*

These premium verification systems operate across platforms through proprietary means, making it a seamless user experience for those that can afford it. Meanwhile, public verification relies on time-consuming, multi-step processes that many users simply abandon out of frustration or impatience.

However, underneath the surface, the organizations that develop and deploy these verification technologies exercise more sophisticated forms of information control. Premium platforms still manipulate feeds to maximize engagement and promote content aligned with their corporate values, and dissenting voices can be effectively silenced by flagging them as "potentially inauthentic," creating a paradox where improved verification enables more covert censorship. The new techno-oligarchs function as de facto information gatekeepers, determining which perspectives receive a stamp of approval.

Digital Literacy has transformed into an essential survival tool for those who cannot afford to pay for these services. Students without access must develop sophisticated skills to negotiate fact from fiction in an increasingly deceptive web *(**Driver: Trust Splitting**,* *literacy becomes a buffer between skepticism and overconfidence)*. Public school curricula struggles to keep pace with the rapidly evolving synthetic technologies, creating a permanent disadvantage for students relying on public education.

In 2034, many Ivy League schools began requiring papers to be submitted through Premium VerifyScholar ($189 per semester for students). They claimed it was about "academic integrity," in order to determine the authenticity and verifiability of submissions, yet for students from lower-income backgrounds, this represents another financial hurdle in an already expensive educational landscape. Ironically, this means wealthy students face stricter limitations on using generative AI in their work, as its use is easily detected in verified environments, while less privileged students increasingly rely on AI assistance to compete academically, conversely also diminishing their cognitive growth *(**Driver: Relationship Quality Transformation**, learning habits shift effecting our ability to connect).*

Knowledge Acquisition now operates through financial gates at every step. Academic journals require expensive verification services both for researchers to publish and for readers to access "authenticated content." This creates financial dependencies throughout the knowledge pipeline, where those without resources face larger barriers to accessing credible information.
We've come full circle, with privileged institutions reclaiming their role as exclusive knowledge gatekeepers (a dynamic the early internet briefly disrupted before monetized verification rebuilt these walls) *(**Driver: Reality Construction**, knowledge access determines reality construction).*

The mechanisms of **Credibility Assessment** have been largely privatized, with proprietary algorithms requiring excessive personal data to determine credibility scores, applied only to paying customers. These systems create biased credibility systems controlled by corporations with minimal transparency requirements. This gatekeeping particularly impacts voices from marginalized communities.

Users without premium verification find their content flagged more frequently for "additional verification needed" that effectively buries their perspectives. This discrimination creates a self-reinforcing cycle where already privileged voices maintain their soapbox while others are effectively muted *(**Driver: Social Signal Manipulations**, credibility systems reinforce old hierarchies).*

The **Social Impact** of this verification divide on the web extends far beyond information access and reshapes social dynamics. Digital verification status has become a social signifier that can determine economic opportunity, romantic prospects, and even physical access to spaces.

Dating apps now prominently feature verification tiers in user profiles, with many premium users filtering out potential matches who lack similar verification credentials. Perhaps most troubling is how verification status has begun reshaping physical access. Restaurants, clubs, and event venues, in an effort to maintain exclusivity, have adopted scanning digital verification credentials; not for fear of inauthenticity, but for the means to automatically cross-check if their credentials line up with a network of their preferred clientele.

These verification barriers have accelerated social sorting, with relationships increasingly forming within verification networks. When this digital status determines which physical and digital spaces you can access, social circles naturally conform to these artificial boundaries, creating exclusive tribes that further fragment society *(**Driver: Relationship Quality Transformation**, further fragmentation of society based on privilege and access divides).*

Dominant **Tools and Technologies** in the verification landscape include quantum-enhanced authentication algorithms, excessive biometric verifications, and cross-platform protocols owned by major tech corporations. These technologies prioritize security over privacy, requiring extensive personal data access to function effectively *(**Driver: Technological Verification Arms Race**, enhanced systems mean invasive trade-offs).* In order to maintain authentication, users are required to surrender all kinds of data including behavioral patterns, keystroke dynamics, and even emotional responses detected through facial scanning. More critical services may even require full body scans and finger pricks.

Privacy and Security Systems operate on tiered models, not unlike technological security systems of yore. However, as synthetic technologies and cyber-attacks evolve dramatically, the need for a paid service on top of hardware is necessary to effectively scour the web safely. Those that can afford it receive both robust security and relative privacy protections, while basic users face a brutal trade-off: surrender extensive personal data or accept significant vulnerability to synthetic threats... without the guarantee that data won't eventually leak ***(Driver: Reality Construction**, the blurred lines between surveillance and authenticity reconstructs our behaviours and perception of authenticity)***.

Premium communication channels enjoy encrypted systems, with authenticated participants, and high-level threat monitoring. Meanwhile, basic users navigate compromised public channels with minimal protection against synthetic manipulation, creating a digital environment where skepticism is the norm.

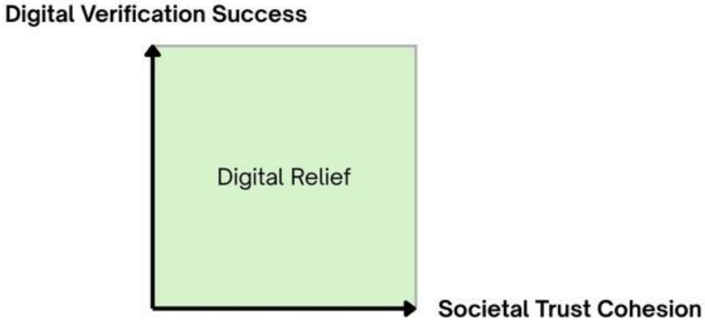
Governance and Policy approaches struggle to address this inequality in a landscape dominated by our techno-oligarchs, as the power and capital they wield shape the very policies meant to govern them. When the FCC established its Verification Standards Committee in 2030, six of eleven appointed members had significant ties or investments with tech companies who own these verification technologies, creating an obvious conflict of interest that fails to hold these companies accountable ***(Driver: Webs with Borders,** ineffective oversight due to privatized internet governance)***.

Some jurisdictions mandate minimum verification standards for essential services, but these baseline protections consistently lag behind evolving synthetic threats, as top technical talent gravitates toward higher paying private companies.

The implications of this verification inequality raise questions about democratic participation itself. How can we maintain civil and fair democratic processes when citizens no longer share access to a common information environment, or have their voices diminished if not aligned with those of the platform?

7.2.3. **Scenario 2:** Digital Relief

(Digital Verification Success × Societal Trust Cohesion)



By 2035, breakthrough technologies in cryptographic verification, advents in quantum computing and collaborative governance systems have created digital environments where verification has become reliably accessible to most users. However, it required something far more challenging than technological advances, it required unprecedented collaboration between technologists, civil society, and governments worldwide *(**Driver: Webs with Borders**, mediated through cross-sector cooperation).*

Trust Formation hasn't returned to the days before synthetic content flooded our screens but rather integrates systems that blend technological verification with a healthy skepticism, buoyed by strong digital literacy skills. The 2031 Global Digital Literacy Initiative marked a turning point, creating standardized approaches to information evaluation internationally. Now, students learn these frameworks alongside other critical subjects, while regular public campaigns help older generations navigate evolving standards *(**Driver: Trust Splitting**, countered by shared literacy and collective trust).*

These new frameworks have created collaborative methods for establishing confidence across diverse sets of communities. The divisive information bubbles that grew some one to two decades ago, have gradually given way to practices that bridge ideological divides, citing varying competing sources and adjusting to degrees of certainty and credibility. This ultimately creates digital spaces where disagreement can occur with a foundation of shared perspectives *(**Driver: Reality Construction**, supported by more widely adopted pluralistic values).*

Verification Practices have democratized through an unexpected alliance between open-source advocates and corporate platforms. The turning point came after the catastrophic 2029 Financial Data Breach, when public outrage forced a fundamental reconsideration of data sovereignty. The result led to regulatory bodies and governments forcing the option of open protocols across platforms that now allow users to see verification levels across platforms, providing consistent indicators of content and identity credibility *(**Driver: Data Sovereignty Movement**, new standards replace platform control and extraction-based models).*

These standards continue to implement "cross-contextual verification", applying different levels of authentication depending on the situation. Critical services like banking and healthcare utilize rigorous verification, while casual social interactions employ a lighter touch approach that doesn't burden everyday experiences. When you're chatting with friends, you'll see basic verification indicators, but when you're reviewing healthcare information, the system automatically elevates verification requirements.

However, these practices have not come about without trade-offs, particularly regarding privacy. While anonymous browsing remains possible, meaningful participation in social platforms typically requires surrendering some privacy to verification systems. Many users accept this exchange, viewing decreased anonymity as a reasonable price for increased authenticity and participation in the digital world.

Digital Literacy has evolved to a fundamental skill. Curriculums at all levels now incorporate these skills, with particular attention to helping students understand both the capabilities and limitations of these authentication systems.

Regular public campaigns help older generations adapt to evolving verification practices, while workplace training ensures verification skills remain current throughout professional careers. More collaborative and community-based initiatives, have financially incentivised tech-savvy teenagers to pair with senior citizens for digital literacy sessions. These sessions emphasize critical thinking alongside technical skills, teaching citizens to interpret indicators while maintaining appropriate skepticism. This in turn has created more resilient digital communities that better resist manipulation even as deceptive technologies continue to evolve.

Knowledge Acquisition has been transformed by the introduction of provenance systems that track content creation and modification history, paired with ongoing digital literacy efforts, allowing users to better assess information origins and validity. Provenance mechanisms now provide a transparent lineage for digital information, showing who created it, how it's been modified, and which verification systems have evaluated it *(**Driver: Technological Verification Arms Race**, temporarily stabilized by provenance tracking and digital literacy efforts).*

These provenance systems work alongside redesigned algorithms (that were restructured after the 2029 crisis) to prioritize verifiability over engagement, making information quality more important than its ability to trigger emotional responses. Platform recommendations now come with explicit explanations, showing why content appears in your feed and the ability to curate said feed further.

These systems are used by governmental services to ensure warning messages reach effected communities. During the 2032 PN-195 outbreak, information about the virus and necessary actions, spread quickly and the public felt more trustworthy that this was an official, government communique, allowing coordinated public health responses that reduced the transmission rates of the virus compared to previous outbreaks.

Credibility Assessment has evolved into multi-layered approaches combining technical verification with community-based reputation systems. While these mechanisms have significantly improved information quality, they've created new challenges for diverse voices lacking established credibility markers or an “in” to a community.

Traditional expertise still carries substantial weight in these systems, creating potential barriers for marginalized perspectives. When elders from indigenous communities initially struggled to gain credibility markers on topics such as climate change, despite their valuable environmental knowledge, it highlighted how credibility frameworks can inadvertently reinforce existing beliefs and knowledge structures.

In response, civil society organizations have responded by developing alternative credibility frameworks that recognize different forms of expertise and experience. This provides pathways for traditional knowledge, lived experience, and community-based expertise, creating more inclusive information ecosystems that value diverse forms of knowing. However, as users now start to apply different knowledge frameworks, a divide in credibility online is starting to form... *(**Driver: Social Signal Manipulations**, softened through community assessments but not eliminated).*

The Social Impact of open-source verification extends beyond information quality to broader social cohesion. As digital spaces have become more reliably authentic, public trust in shared information has gradually recovered, rebuilding foundations for collective action and democratic participation. However, this renewed trust comes with increased accountability for users, as reduced anonymity online means actions have consequences in both digital and physical realms.

The relationship between humans and synthetic systems has also evolved through clear boundaries and disclosure requirements. Engaging with generative AI now includes mandatory health warnings, with special protections for users under 18, who cannot legally use these systems without parental supervision. These guardrails reflect growing recognition that synthetic interaction, while valuable in specific contexts, requires clear delineation from human connection.

Tools and Technologies have aided in the verification landscape utilizing quantum-resistant cryptography and advanced authentication systems that make manipulation immediately detectable. Rather than attempting to eliminate synthetic content entirely, these technologies focus on mandatory labeling that prevents deception, recognizing that synthetic content itself isn't inherently problematic, the harm comes from misrepresentation *(**Driver: Technological Verification Arms Race**, diverted toward transparency rather than elimination tactics).*

The technical infrastructure supporting these systems has created safer digital environments, but at the cost of significant environmental impacts. The energy consumption of these novel technological systems remains concerning despite efficiency improvements, creating tension between continued use of digital technologies and environmental impact *(**Driver: Web 4.0, 5.0, 6.0...**, introducing new tensions between future architectures and sustainability).*

Privacy and Security Systems have evolved to minimize unnecessary data collection while enabling verification. Zero-knowledge proofs allow authentication without exposing sensitive information, while decentralized systems give users control over credential sharing their credentials.

However, the tension between verification needs and privacy protection remains unresolved, particularly on public platforms. While private messaging can utilize end-to-end encryption with minimal verification requirements, participation in public discourse typically requires more substantial identity disclosure.

Governance and Policy approaches have achieved significant international coordination on technical standards, recognizing that verification and cybersecurity challenges transcend national boundaries. International frameworks have developed to establish common protocols still allowing regional implementation variations that respect cultural and legal differences; while maintaining accountability for bad actors across borders *(**Driver: Webs with Borders**, governance reimagined through coordination)*.

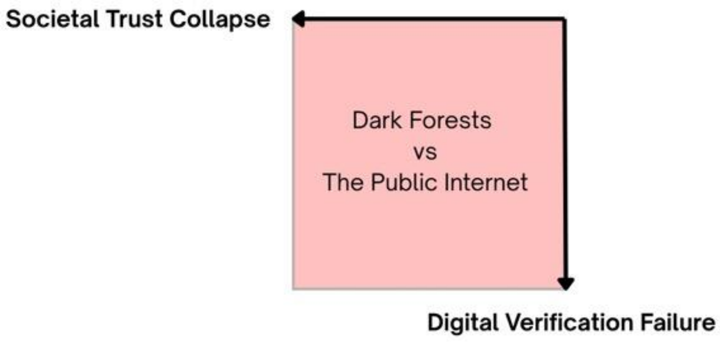
Regulatory approaches focus on outcomes rather than specific technologies. This allows continuous technological evolution while maintaining accountability for those perpetrating harms as outlined by these laws. When Meta failed to implement adequate synthetic user labeling in 2030, significant penalties were levied to the company, with three key members of the organization charged to appear before the International Criminal Court for "cyber-related crimes".

Local governance bodies now utilize a multi-stakeholder approach encompassing civil representatives, technologists, and government representatives, in order to create more responsive frameworks that maintain verification and the safety of the digital realm as a public good, rather than a commercial product.

As we navigate this digital renaissance, the challenge is no longer the anticipated effects of the emergent technologies and our digital world (as our current world so eagerly focuses upon), but rather can this new environment give way to a focus, collaboration and agreement about a much more critical need for our survival: the significantly eroding environment, exacerbated by the energy of these new technologies.

7.2.4. Scenario 3: Dark Forests vs. the Public Internet

(Verification Failure × Trust Collapse)



By 2035, verification technologies have consistently failed to keep pace with bot proliferation and sophistication, creating a digital world divided into two distinct realms: the invitation-only “Dark Forests” and the increasingly vulnerable “Public Internet.” This division represents more than just different user experiences, it reflects a fundamental fracturing of societal trust and shared reality.

Trust Formation has evolved in dramatically different paths in these separate digital ecosystems. Dark Forest communities have largely abandoned technological verification, instead developing elaborate social verification systems based on personal vouching and reputation *(**Driver: Retreating to the Dark Forests,** formation of trust enclaves in response to verification failure).* These communities prioritize human connection and known networks over sole technological solutions that have repeatedly proven inadequate.

Meanwhile, the public internet has become a landscape of profound uncertainty. Users navigate environments where identifying the authentic from the synthetic has become virtually impossible through technological means alone *(**Driver: Technological Verification Arms Race**, synthetic content outpaces detection systems).* This uncertainty creates a dangerous split in user behavior: some develop extreme skepticism that rejects even valid information, while others place unwarranted confidence in unreliable sources that appear just as credible on the public web *(**Driver: Trust Splitting,** divergent trust in high uncertainty environments).*

The Central Bank of Thailand's collapse in 2034 illustrates this vulnerability. What began as a market rumor, perpetrated by large-scale bot networks and even verified by three respected news outlets (whose systems had been compromised), triggered a catastrophic bank run with enormous economic consequences (***Driver: Reality Construction****, breakdown of reliable reality signals in critical systems).* This incident is not uncommon, as financial systems have become increasingly susceptible to synthetic attacks carried about by malicious bot networks. The result? Physical cash is increasingly becoming king... with gold and goods soon on the horizon...

This trust split between public and private digital worlds extends beyond online interactions to shape even physical world relationships. People increasingly view the physical world through the lens of their digital communities. When neighbors belong to different information ecosystems, their shared reality fractures along those same lines. How can you agree on local policy when you can't even agree if the mayor's speech was real?

Verification Practices have shifted from technological solutions to social verification mechanisms. Respected “Dark Forest” communities implement multi-layered entry processes that typically include personal references, attendance at physical meetings, credential checks, and even probationary periods to better establish trustworthiness *(**Driver: Verification Arms Race,** tech failure leads to localized, physical alternatives).*

One popular online finance community requires new members to solve verification puzzles that change regularly based on cultural references and memes, engage in video interviews with established members, and maintain a six-month probationary period before gaining full access. It's exhausting, exclusive, and surprisingly effective.

The public internet continues to deploy increasingly sophisticated verification technologies (e.g. quantum-enhanced CAPTCHA's, advanced pattern recognition, etc.) but these systems are routinely circumvented. Each new technological solution is met with adaptive counterstrategies, creating a verification arms race that protective technology consistently loses. This year's new buzz word is: "Quark-scale Computing." *(**Driver: Technological Verification Arms Race**, innovation consistently undermined by malicious actors)*

These opposing digital ecosystems have escalated social divisions further. The verification requirements for these "Dark Forest" communities, while effective, favor those with existing social connections, educational credentials, and the resources to navigate these ever-changing entry processes; reinforcing existing privilege structures.

Digital Literacy has transformed into an essential survival skill. Educational institutions now formally teach digital literacy, but with varying quality and effectiveness. Private schools employ former and current cybersecurity experts to train students in pattern recognition and verification practices, while public schools struggle with outdated curricula and limited resources that often lag behind current tech *(**Driver: Relationship Quality Transformation**, uneven social development in increasingly untrustworthy digital environments).*

This disparity creates a vicious self-reinforcing cycle, in which the privileged receive better access to quality education, improve their means of identifying deception, gain access to the private and exclusive communities (which further improves their skills through peer learning), and pull even further ahead. Meanwhile, those with limited resources remain vulnerable in public digital spaces, falling prey to increasingly sophisticated scams and manipulation, constantly negotiating what is real and what is not, increasingly abandoning the web as a resource for information and connection.

Knowledge Acquisition now operates through parallel systems that rarely intersect. Dark Forest communities maintain their own knowledge repositories (private wikis, verified research archives, expert-curated news feeds) creating information ecosystems that are relatively reliable but increasingly isolated *(**Driver: Web 4.0, 5.0, 6.0...**, fragmented due to architectural pressure on public web).* Public knowledge resources have become poisoned by synthetic infection. Wikipedia collapsed under the weight of synthetic edits in 2031, replaced by dozens of competing encyclopedia projects, each reflecting different reality tunnels and each susceptible to similar attacks without proper support from each other. Academic journals maintain private circulation networks, accessible primarily to subscribers. The result resembles a knowledge feudalism. Information quality correlates directly with access privileges, reversing decades of democratized knowledge that the early internet promised.

Credibility Assessment mechanisms have diverged dramatically. Dark Forests rely on multi-layered community assessment processes such as reputation systems and consistent cross-referencing against verified sources within their communities. These systems can be impressively accurate but often reinforce community biases *(**Driver: Social Signal Manipulations**, community-specific signals trusted over public credibility).*

Meanwhile, public internet users develop personal verification methods out of necessity. "Only trust videos with unbroken background audio. If it breaks, you've got a fake." "Check and see if the guy's earlobes move naturally." "Ask your neighbour!" However, these methodologies offer limited protection against increasingly sophisticated synthetic content.

The Social Impact of this growing split reaches far beyond information quality. Community divides have sunk deeper as "reliable" information becomes scarce and protected. Relationships form primarily within similar online communities, creating echo chambers that further fragment our shared reality *(**Driver: Trust Splitting**, social fragmentation via divergent trust;*

***Driver: Reality Construction**, breakdown of shared reality between even proximal communities).* The global social cohesion necessary for addressing challenges from climate adaptation to pandemic responses has also weakened dramatically. How can we collaborate when we can't even agree on basic facts?

Tools and Technologies for verification have diversified as centralized solutions repeatedly fail. Private communities develop their own specialized verification approaches tailored to their specific needs, often combining physical verification with eventual technical assistance *(**Driver: Webs with Borders**, localized solutions emerge in lieu of governance).* While these approaches work for private communities with access and resources, they don't scale to members of the public and marginalized.

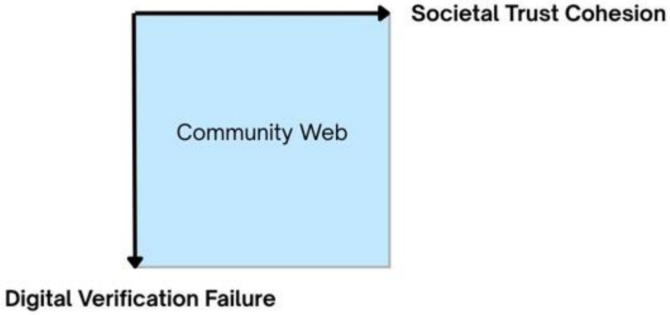
Privacy and Security Systems face seemingly contradictory pressures. These growing Dark Forests require substantial personal disclosure for membership while attempting to maintain stronger external security boundaries. Users surrender privacy in order to engage in their digital communities, in exchange for stronger protection from external threats (submitting to processes that would have seemed invasively intrusive a decade ago). Meanwhile, the public internet, riddled with bots, has users playing Russian Roulette with their data, increasingly susceptible to scams, identity theft and malware exposure.

Governance and Policy approaches have fractured in the age of a regressed web. Private communities implement internal governance systems with their own rules for content moderation and verification standards with minimal external oversight. National governments struggle to address synthetic proliferation in public digital spaces due to challenges in enforcement when bad actors cross jurisdictional boundaries *(**Driver: Webs with Borders**, enforcement falters across fractured internet governance).* International Acts legislating the deployment of bots and synthetic entities has fallen on deaf ears, as these bad actors routinely spoof their identity and location, and as geopolitical tensions have hit an apex, with national governments refusing to hold their citizens accountable if accused by other nations.

The digital divide of the 2020s has evolved dramatically into a verification divide that only reinforces and amplifies our existing social inequalities. Without shared information environments, democratic processes themselves face existential challenges. How can citizens make collective decisions when they no longer share a common understanding of what is *real* and what is *not?...*

7.2.5. **Scenario 4:** Community Web

(Verification Failure × Trust Cohesion)



By 2035, we are still losing the battle against synthetic entities, however, we have developed collective approaches to managing the chaotic web that now utilize shared information frameworks and in turn begin to foster a stronger sense of social cohesion online and off.

Trust Formation online has undergone a fundamental transformation. After years of false promises from tech companies claiming their newest advent would curb bad bots, verify users with certainty and be able to detect misleading content, society has finally accepted the humbling truth that perfect technological verification *isn't coming*. What has grown in popularity instead, are community-based approaches to establishing reasonable trust without requiring absolute certainty *(**Driver: Retreating to the Dark Forests**, reframed as community resilience rather than isolation).*

These frameworks embrace probability rather than certainty. When you encounter information online in 2035, verification indicators do not claim to be definitive, rather they show confidence ranges based on multiple community assessments. The days of "real" versus "fake" have given way to more nuanced systems that help people adjust their confidence levels based on context, source patterns, and community evaluations.

This is turn has had significant effects in the ways by which social norms have also evolved. People have learned to live with a degree of uncertainty and operate with a more pluriversal sense of the world and each other, recognizing that there are many different ways of "knowing". *(**Driver: Reality Construction**, amended through more popular adoption of pluralistic worldviews).*

Verification Practices have shifted to distributed verification methods that leverage collective intelligence. When the Global Verification Initiative's: Quantum Computing Authentication System (GVIQCAS) failed to detect even simple, unsophisticated synthetic actors back in 2029, it forced a fundamental reconsideration of utilizing purely technological approaches *(**Driver: Technological Verification Arms Race**, deprioritized in favor of human-centered alternatives).*

Content online now typically undergoes assessment through multiple overlapping communities, creating reliability ratings that reflect a diversity of perspectives. This approach builds on the foundation laid by Twitter's Community Notes in the 2020's, which demonstrated how collective assessment could effectively identify misleading content even when automated systems and platform administrators failed. The framework has evolved dramatically since then, expanding from simple binary flags to assessments that incorporate multiple dimensions of reliability.

Growing from early experiments with decentralized web annotation systems, open protocols now allow community assessments to appear as a layer atop any content on the web. This approach emerged from the early "Overweb" concepts of the 2020's, creating infrastructure that functions as a public utility rather than a commercial service *(**Driver: Web 4.0, 5.0, 6.0...**, realized as decentralized technologies explode in popularity and necessity).* This also allows communities to contribute without requiring platform-specific integration.

Digital Literacy has expanded beyond technical skills to teach and encourage contribution to community assessment systems. Educational initiatives like the Digital Citizenship Curriculum, now standard in most schools, teach students how to interpret authenticity indicators and contribute meaningfully to collective processes, unlike earlier approaches that emphasized individual evaluation in isolation *(**Driver: Social Signal Manipulations**, mitigated through shared learning and interpretation frameworks).*

Knowledge Acquisition online now operates through information ecosystems built on transparent provenance tracking. The Web of Trust framework, evolving from early blockchain-based provenance tracking, now maintains content origin trails while community assessments provide evaluation contexts.

Wikipedia's transformation in 2031 exemplifies this approach. After struggling with bad actors repeatedly editing their webpages, it implemented a community verification layer that shows how different specialist groups have assessed content reliability. Rather than claiming an absolute truth, entries display layered assessments allowing readers to make informed judgments.

Credibility Assessment mechanisms now blend individual judgment and community consensus into layered systems. Built off the backs of the *W3C Credible Web Community Group*, we now have established standards for displaying these assessments across platforms *(**Driver: Trust Splitting**, softened through availability of multiple perspectives).*

The embrace of knowledge pluralism online has begun to influence how societies approach complex challenges offline. For example, climate adaptation strategies increasingly incorporate indigenous knowledge alongside scientific assessments.

The Social Impact of these community systems has helped renew a sense of social cohesion. Rather than fragmenting into isolated reality bubbles, society has developed shared methods for navigating the web together by enabling cross-community communication about its reliability *(**Driver: Relationship Quality Transformation**, realigned towards building trust through cooperation).* This extends offline as people begin to both feel a renewed sense of a shared reality, as well as the secondary effects of engaging with multiple points of view that allow for less barriers to social cohesion offline.

Tools and Technologies now focus on integrating and negotiating human assessment rather than attempting to replace it. Rather than claiming to determine authenticity itself, current tools and frameworks help human assessors identify potential manipulation through unusual content patterns or user activity. This new process allows for decentralized assessments that compile user judgments, without sole focus on a single perspective.

Privacy and Security Systems now maintain greater boundaries between verification needs and privacy protection. After early community verification systems raised privacy concerns, advances in decentralized technologies now minimize unnecessary data collection. Zero-knowledge authentication now allows verification of credentials without revealing unnecessary personal data *(**Driver: Data Sovereignty Movement**, implemented via collective governance).*

Governance and Policy approaches to these community verification systems vary dramatically across different political contexts. The decentralized nature of these systems has created fundamental tensions with authorities accustomed to more centralized control. In democratic societies, governments have gradually accommodated these systems; however, even in these contexts, security agencies have expressed concerns about verification systems operating outside of direct government oversight.

Authoritarian regimes have taken much more aggressive approaches to suppressing community verification infrastructures. Russia, China and Iran who have maintained sovereign intranets, have explicitly banned web overlay technologies, maintaining centralized control on their respective webs. However, despite these bans, digital dissidents maintain underground communities that seek collective criticism of their nations.

Hybrid models have also emerged that attempt to balance community verification with state oversight. India's Digital Information Act of 2023 has been updated in order to provide means for community verification systems, but requires registration and accountability measures, with minimal privacy from government authorities, threatening those that may speak out against their government *(**Driver: Webs with Borders**, still contested across global regimes).*

Together, this world exemplifies how rather than relying solely on institutional or technological authority, societies are learning to navigate the digital world through pluralistic and participatory efforts. While challenges remain, especially across political regimes, this scenario offers a glimpse into a world where collective assessments of credibility and verification may reshape both the architecture of the web and the social fabric it underpins.

7.3. Reflections & Insights from Scenarios

Scenario 1: Pay for Trust

This scenario imagined a future where verification technologies succeed in the fight against synthetic dominance, but have since been heavily monetized, creating deep asymmetries in who can access trustworthy information and participate in "verified" digital spaces. Trust, in this future, becomes a commodity, with premium users gaining authority over knowledge and information, acting as 'knowledge barons', while others remain trapped in uncertainty and skepticism. These dynamics strongly point to the need for platforms that center human presence and values over bots, extraction, and engineered influence. Platforms that explicitly design for authenticity online as a public good, rather than a luxury good. The scenario also highlights the dangers of privatized credibility systems that exclude marginalized perspectives, pointing toward the necessity of measures such as standardized credibility labels cross-platform, as well as provenance tools to decipher content origins in order to better assess the authenticity and content history of these users and their claims. The educational disadvantages depicted in this world, where less affluent students rely on tools that further reduce cognitive development, also reinforce the importance of early and equitable AI/media literacy education. In this vein, there is also potential for public awareness campaigns to mitigate divides and educate the broader public before even more harm can be done.

Scenario 2: Digital Relief

Digital Relief portrays a more optimistic trajectory of the worlds that could be. Where technologies meant to curb, or more accurately identify synthetic entities on the web, succeed and are widely accessible thanks largely in part to enhanced global collaboration. This scenario envisions the promise of multi-stakeholder governance structures actively shaping technological solutions, embedding human safety, civic input, and shared values into the foundations of AI design. Additionally, the renewed public trust seen in this scenario does not arise solely from ongoing technical solutions but from collective resilience fostered through ongoing public education and cross-generational training. The balance struck between verification and privacy here further justifies the need for authentication methods that prioritize privacy, such as zero-knowledge proofs, and more broadly, the continued importance of human-centered system development that prioritize integrity over engagement**.**

Scenario 3: Dark Forests vs. Public Internet

In this more dystopian world, verification systems have failed, and society splits between exclusive, socially verified enclaves and the ongoing, chaotic, public web. The fragmentation of reality and the proliferation of synthetic content in ungoverned digital zones point to the urgent need for more cross-platform collaboration and real-time content authentication tools, in order to better identify synthetic agents and content. The survivalist nature of digital literacy in this world, in which only the well-connected can protect themselves from deception, makes a powerful case for expanding education initiatives to advocate for digital literacy and resilience. This includes, not just technical literacy, but also *emotional* and *behavioral* components as well in order to combat the emotional manipulation of algorithmic content. The unequal access to reliable knowledge and the creation of insular knowledge environments in this world emphasizes the urgent need for independent oversight bodies and laws protecting cognitive liberty; not only in terms of content moderation, but to safeguard the infrastructures through which people form beliefs. The inability of governments in this scenario to address synthetic threats across borders also presses the value of ongoing international cooperation**,** including the development of international laws and rapid alert systems for cross-border cyber-attacks. While such collaboration may seem unlikely in an era of geopolitical fragmentation, the principle remains: a rising tide lifts all boats.

Scenario 4: Community Web

The Community Web effectively reflects a grassroots response to technological failures, in which people construct shared trust through community driven verification and knowledge practices. It's success directly points to the need to develop more crowdsourced fact-checking systems and the development of content assessment tools that do not depend on centralized platforms. The normalization of pluralistic worldviews in this scenario, those that encourage multiple perspectives and inputs on topics, also point to the potential to reframe current educational efforts to more actively cultivate curiosity and humility in order to prevent further divisiveness. Children raised within these paradigms may become more open-minded and less prone to binary thinking, possibly reducing divisiveness in both their offline and online interactions. Similarly for platforms, their architectures can actively facilitate layered, community-driven credibility judgments giving a means to better assess credibility in digital environments. The emphasis on local knowledge, peer-based learning, and provenance in this world further validates investing in decentralized knowledge systems and public-interest driven data protocols. These measures can help shift the internet toward serving the public good, rather than continuing to function as a system of extraction. Lastly, this scenario exemplifies the urgent need to protect our cognitive liberty and uphold the right to form our beliefs without manipulation, especially when verification in this world is negotiated socially rather than technologically.

7.4. Final Remark on Scenarios

Exploring the divergent scenarios from: *Pay for Trust,* where authenticity becomes a commodity and trust is bought and sold; to *Digital Relief*, a future of quantum computing and collective coordination; to *Dark Forests vs the Public Internet* where we continue to retreat into our digital enclaves or face the chaos of the wild, wild, web; to a *Community Web* of local networks rebuilding trust from the ground up; each scenario highlights a challenge, escalating with each waking day: the current and potential erosion of our realities from synthetic text, media, and personas, highlighting the urgent need to reinforce human verification, cognitive liberty, and social connectedness as pillars of resilience.

8. Outcomes & Discussion

"I am even more deeply concerned about the future of our democracy now than I was in mid-2016, when I was one of the few raising the alarm about social media creating an explosive breeding ground for misinformation. Facebook and its brethren have begun to take this threat seriously, but the next threat—the distortion of reality itself—is fast approaching." -Aviv Ovadya (2018), founder of the AI & Democracy Foundation

The scenarios presented in the previous chapter were not just speculative tools. They serve as critical sensemaking devices that helped reframe the central questions of this research. Initially anchored in an inquiry into the plausibility and implications of the Dead Internet Theory, this study has evolved to incorporate a broader examination of how synthetic content, emergent AI technologies, and automation are reshaping the very construction of reality.

As the scenarios unfolded, they exposed not only the shifting terrain of trust and verification, but also the deep entanglement between technology and our social and cognitive systems. What began as an exploration of bot activity and synthetic interactions online now reveals a more complex and urgent set of transformations, where the boundary between physical and digital, authentic and artificial, signal and simulation, is increasingly unstable.

This chapter reflects on what the scenarios, and previous insights, have revealed across system levels, from cognitive erosion and fragmented social trust to the infrastructural and governance failures underpinning these trends. In doing so, it bridges the foresight process to the recommendations that follow.

8.1. From Digital Skepticism to Existential Threat

"Deepfakes have already put a big dent in reality, and it's only going to get worse. In setting after setting, we will find it impossible to distinguish between the natural and the synthetic. ... As we snuggle closer to these intelligences it will be increasingly difficult to distinguish who (or what) did what. ... AIs will successfully emulate core human traits." - Jerry Michalski, longtime speaker, writer and tech trends analyst (as cited in Anderson & Rainie, 2025, p.16)

What began as a fringe conspiracy theory, that all our interactions and information on the internet are perpetrated by synthetic actors and content, has evolved into a profound inquiry into how synthetic entities, automated systems and the power of artificial intelligence, are fundamentally reshaping our relationship with reality itself. This research points to a troubling trajectory: What was once a conspiracy, seemingly confined to digital platforms, has become a reality that has steadily infiltrated our critical systems, our social relationships, and now threatens to transform our very construction of reality, both shared and individual.

At the microsystem level, we observe current transformations in trust formation, digital literacy, and knowledge acquisition, which suggest we are approaching what Ovadya (2018) had termed an "Infopocalypse", the catastrophic failure of the marketplace of ideas. Where information that isn't verified through *face-to-face human interaction* becomes increasingly suspect. This represents not merely a crisis of information, but a fundamental shift in how we establish what is real.

Within the mesosystem, verification practices and credibility assessment mechanisms that traditionally bridged digital and physical contexts are increasingly failing. Ironically enough, we are witnessing the potential reversion to physical verification as a response to the collapse of digital trust in the age of technological sophistication. Meanwhile, social relationships are transforming significantly as synthetic entities alter human connection expectations and hijack cognitive processes. Current research is also beginning to reveal concerning developmental implications as new generations interact with synthetic entities and the subsequent effect on their critical cognitive capabilities (Gunadi, & Lubis, 2023).

Moving to the exosystem, we see how tools and technologies that once served human needs are increasingly shaping human behavior. Our research revealed how IoT proliferation creates environments where synthetic entities inhabit everyday devices, not merely passively collecting data, but actively curating our exposure to information, products, and ultimately, our perception of reality itself. This escalates as intelligent environments increasingly determine what information reaches us, which options seem available, and how we understand our surroundings; suggesting that the last vestige of unmediated reality: our physical environment, is now under threat.

This technological infiltration may grow even more profound with each technological evolutionary step. Wearable technologies position themselves directly on our bodies, augmented reality systems overlay digital information onto our perception of physical environments, and virtual reality replaces visual and audio sensory inputs with synthetic alternatives altogether. Our horizon reveals even *more* profound technological integrations, through cybernetic technologies, *a la* Neuralink, that utilize direct brain-computer interfaces. Each of these advancements has the potential to further obfuscate the boundary between the creation of our individual realities and a technologically mediated experience, calling into question not only our ability to maintain a *shared* reality but our capacity to distinguish *our own perceptions*.

This progression culminates at the macrosystem level with regulatory approaches that struggle to address this phenomenon as it transcends jurisdictional boundaries. Current governance frameworks in our increasingly fractured geopolitical climate, diverge between democratic and authoritarian states. Simultaneously, techno-oligarchs are increasingly positioning themselves as de facto regulators, implicating themselves within formal decision-making authorities while shaping the very technologies requiring governance (Here's looking at you Elon).

8.2. The Transformation of our Realities

"AI's ability to curate everything – from entertainment to social connections – could lead to highly personalized but isolated 'realities.' This is a trend I call the rise of 'Citizen Zero,' where people are living only in the present: disconnected from a shared past, not striving toward any common vision of a future. Human interactions may become more insular as we retreat into algorithmically optimized echo chambers. And, as we already know, millions of pages of research, footnotes and opinion are disappearing daily from the internet whilst the Tech Platforms reach into our phones and erase photos or messages whenever they want – perhaps even without our knowledge – and AI is only going to make that more scalable." - Tracey Follows, CEO of Futuremade a UK-based strategic consultancy (as cited in Anderson & Rainie, 2025, p.16)

All of the factors discussed thus far culminate in threats to something more fundamental than information accuracy or technological ethics; it challenges *how* humans construct reality itself. As Echterhoff et al. (2009) explain, in their work on social identity theory and shared reality, humans commonly determine what is real through social verification of inner states about the world; and Hogg & Rinella (2018) further this by elucidating that we establish confidence in our perceptions, our judgments, and our evaluations through *interaction with others*, creating what they describe as social identity processes that produce inter-subjectivity and a sense of shared reality. Yet our analysis reveals how synthetic entities are increasingly disrupting this fundamental process.

This research surfaced how artificial social signals created by synthetic user networks make certain viewpoints appear more widely held than they actually are. This manipulation of apparent social consensus directly targets what Hogg & Rinella (2018) identify as a *key motivation* for group identification: "self-uncertainty reduction". When these cues are distorted, the social mechanisms for reality validation are *systematically* manipulated, and reality itself becomes increasingly uncertain.

As our shared reality erodes, we see the potential for even our individual reality to be threatened. As Matta's (2024) research shows, predictive technologies and personalized algorithms can limit cognitive liberty by narrowing information exposure, potentially leading to deterministic thinking patterns that inhibit creativity and motivation. This represents not merely a *continuation* of existing problems, but a *fundamental transformation* in how reality is constructed at the individual level.

The mechanisms through which we perceive and make sense of the world are increasingly influenced by artificial systems designed primarily for engagement and commercial interests rather than human flourishing (Petropoulos, 2022; Haleem et al., 2022; Stahl et al., 2021). As these systems go beyond *anticipating* to *shaping* our desires, beliefs, and behaviors, they create personalized reality tunnels that may result in a fragmentation that threatens not just social cohesion, but our capacity for shared understanding.

8.3. Extension to the Physical World

"By 2035 we will be surrounded by AIs: bots that work for you, bots that work with you, bots that work on you and bots that work around you and with each other." – Marina Gorbis, Executive Director of the Institute for the Future (as cited in Anderson & Rainie, 2025, p. 207)

"Physical and digital realities are dissolving, blurring the lines between real and fake, while social trust erodes and shared truths fade… The gap between thought and action are closing with experimental brain-computer interfaces (BCIs), neural implants, and mixed-reality tools, allowing people to control digital environments with a glance or gesture… As virtual and physical realities become inseparable, identity, perception, and social structures are being rewritten in real time." – ANTICIPATE (2025, p. 20), strategic foresight consultancy on Megatrends transforming our world

More concerning currently, is how these phenomena have expanded and infiltrated our physical world and critical infrastructures. Our research identified serious concerns about the interconnection between critical infrastructures and digital networks, creating unprecedented vulnerabilities where synthetic attacks could target essential services. Current cyberattacks already demonstrate the vulnerability of these systems: banking, financial services, government, and public utilities such as energy providers experienced a 55% increase in DDOS attacks over the past four years (Constantin, 2024). With growing sophistication and access to bot networks, these attacks could become more frequent and devastating.

When critical infrastructure systems become compromised, the consequences extend far beyond information manipulation to potentially *catastrophic* physical harm. Water treatment facilities, power grids, transportation systems, and healthcare networks increasingly rely on digital control systems vulnerable to synthetic manipulation (Constantin, 2024; Imperva, 2024a).

Furthermore, the deployment of IoT devices into everyday environments represents a particularly troubling frontier. As our research revealed, we are now moving internet technologies from the cloud into our homes, eroding the boundary between digital and physical environments. This evolution, alongside always-on microphones collecting unconsented data, evaluating human behavioral patterns, and subsequently curating our exposure, represents what Ovadya describes as the "distortion of reality itself" (p.1). Mark Weiser highlighted this threat as early as 1991 in his work *The Computer for the 21st Century,* stating "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it" (Weiser, 1991, pp. 66–75).

Ovadya (2018) furthered that this ongoing threat goes beyond just "fake news" to challenge our fundamental ability to determine whether a world leader is truly ordering a nuclear strike or if that really is our spouse's voice asking for bank information (p.1). We are moving beyond *information* manipulation to *reality* manipulation. The question Ovadya poses is chilling:

Which hurts civilization more: no one believing anything, or everyone believing lies?

This distortion warps both individual perception *and* collective sensemaking. When the mechanisms through which we establish shared reality by social verification, sensory perception, and even institutional authorities, are systematically manipulated, the foundations of social cohesion erode. Communities fragment into epistemic tribes with incompatible versions of reality, making collaborative action on shared challenges increasingly difficult… if not impossible.

8.4. Our Ways Forward

"We may find it hard to distinguish between artificial personalities and real ones. That may result in a search for reliable proof of humanity so that we and bots can tell the difference."- Vint Cerf, vice president and chief Internet evangelist for Google, a pioneering co-inventor of the Internet protocol and longtime leader with ICANN and the Internet Society (as cited in Anderson & Rainie, 2025, p. 179),

In the face of these challenges, this and ongoing research, as well as emerging practices suggest several potential pathways forward. At the individual level, endeavouring to develop enhanced critical evaluation skills becomes increasingly essential. These must consider going beyond technical literacy to include what Martin (2006) emphasizes as the awareness, attitude, and ability to assess information, not just for accuracy, but for intention and origin. As synthetic content becomes more human-like, these skills become a first line of defense in preserving both cognitive autonomy and discernment.

But resilience cannot be built by individuals alone. Addressing these challenges at scale may require, as Kaminski (2019) outlines: regulatory approaches that combine top-down mechanisms with collaborative governance; bringing together public institutions, platforms, civil society, and technologists to shape how we govern synthetic entities. This includes creating *adaptable* frameworks that can evolve alongside emerging technologies.

Ovadya (2018) also highlights a set of interventions that remain increasingly relevant to these challenges and striving to sustain our sense of reality by: monitoring the information ecosystem, fostering responsible research and design, implementing authenticity infrastructures, and ensuring information markets reward *reality* over *misinformation*. These themes inspired and echo across the development of our recommendations in the following chapter; particularly in relation to reforming the current architecture of the web.

Leibowicz's (2025) recent work on synthetic media governance also emphasizes that trust, not only in technical systems, but between the stakeholders involved, will determine whether governance efforts succeed. This research supports this view. Successful interventions must endeavour to establish credibility on multiple fronts, not just in the tools used, but across the social and institutional systems implementing them. These approaches also include striving to design tools that do more than just *signal* whether content is AI-generated but aim to convey *context* and *process*. Some of our recommendations point to features such as credibility indicators, disclosures of content creation or participatory labeling systems, but they also recognize that fostering trust will require a social focus in building norms of curiosity, skepticism, and a shared responsibility around how knowledge is constructed and consumed.

Ultimately, the proposed interventions that follow are not silver bullets, they are system-level levers. Many are already being piloted; others remain speculative, intended to provoke further exploration. But their effectiveness will depend on how we, collectively, choose to act. In navigating our increasingly synthetic realities, the way forward lies in our capacity to proactively construct flexible and human-centered systems that prioritize our safety over our hubris.

9. Recommendations: *This is Where We Could Go Next.*

"The path forward lies not in resisting AI advancement but in consciously preserving spaces for human development and connection. This means designing organizational and social structures that actively value and protect human capabilities, not as nostalgic holdovers but as essential counterweights to AI mediation. Success will require recognizing that human agency isn't just about making choices – it's about maintaining the capacity to shape our individual and collective trajectories in an increasingly AI mediated world." - Lior Zalmanson, a professor at Tel Aviv University whose expertise is in algorithmic culture and the digital economy (as cited in Anderson & Rainie, 2025, p.63)

The following recommendations synthesize the exploration of the foresight inquiry and research project thus far across technological, regulatory, and social domains. Rather than proposing purely technical fixes, they identify possible pathways for reshaping the conditions under which synthetic content and actors emerge, operate and infiltrate our lives. These are not endpoints, but exploratory directions that point to where momentum, capacity, and intervention may be most impactful.

9.1. The Development of Recommendations

The initial set of broader recommendations formulated in response to the foresight inquiry, served as a springboard for developing more targeted measures. These refinements were also guided by insights from the SoTA review, expert interviews, and ongoing inquiries into current policies and emerging advocacy efforts.

The devised proposals were then organized across the neo-ecological systems framework. For example, the general insight of "Community-Based Verification" was scaled into multiple systems. It was introduced at the Microsystem level as a way to rebuild interpersonal trust, and at the Mesosystem level through *Crowdsourced Fact-Checking* and *Cross-Group Exchange*. Similarly, the insight of the need for "Global Norms and Cooperation" were incorporated at the Macrosystem level to reflect international alignment on *Co-Governance Structures* that aim to bridge public, private, and civil stakeholders.

To more comprehensively illustrate the insights gained from each of the four scenario worlds, a consolidated Sankey diagram has been included in **Appendix F.** This diagram maps each future world to the some of the key insights they reveal and serves as both as a summary and a comparative tool. In parallel, the table in **Appendix G** outlines how these insights align with the research's challenge domains and informed the corresponding recommendations. Together, these visuals illustrate key connections between the foresight inquiry and the development of proposed interventions, while acknowledging that they will only partially capture the complexity of the process and analysis.

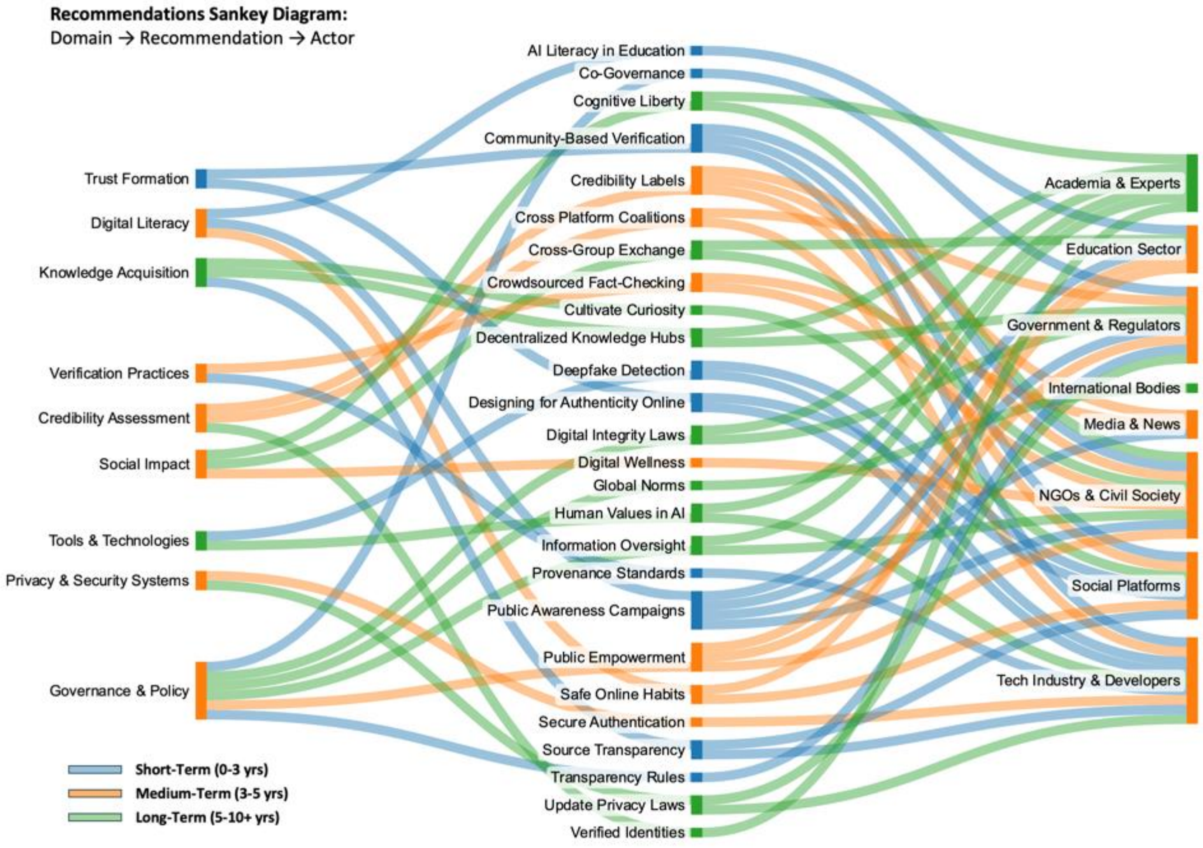
9.2. An Overview of Recommendations

9.2.1. A Comprehensive Recommendations Sankey Diagram

The following recommendations are designed to operate across domains and timelines, supporting both immediate responses and long-term resilience. To ground them in action, each includes key actors (those with the agency or responsibility to respond) and an estimated timeline for implementation (from short-term implementation to longer-term commitments), as exemplified in **Figure 25**. Together, they offer a frame for navigating, mitigating and shaping knowledge environments increasingly mediated by synthetic entities and emergent technologies.

Figure 25

Comprehensive Recommendations Sankey Diagram



Note: This Sankey diagram visualizes the relationship between challenge domains, the corresponding recommendations developed, and the grouped actor categories responsible for implementation (for a full list of the actors involved in these groups refer to **Table 6** *Grouped Actor Categories***.** Flows are color-coded by estimated implementation timeline: blue for short-term, orange for medium-term, and green for long-term. The diagram illustrates how system-level responses span across micro to macro domains and require coordinated efforts across stakeholders and timelines. For closer analysis, a full-page version of this diagram is also included in **Appendix H.**

9.2.2 Actors across the systems

The actors listed in the recommendations, and the groups they were categorized into for the Sankey diagrams, were derived through an iterative process, synthesizing much of the research study up until this point as well as consulting ongoing policy and advocacy efforts.

These actors are not intended as *exhaustive* or *definitive* classifications, nor do they presume complete knowledge of the institutional and sector dynamics involved. Rather, they serve as means to help surface where responsibility or influence may be most relevant. This aims to recognize that implementation often depends on context specificities and institutional intricacies that extend beyond the scope of this study.

9.2.3. Grouped Actors

Considering the breadth of specific actors across systems, the *Comprehensive Recommendations Sankey Diagram* in **Figure 25** and the sankey diagrams that follow **(Figures 26, 27, 28, & 29**) consolidate individual actors into eight broader categories to enhance clarity and readability. **Table 6** (found below) outlines which specific actors are grouped under each category

Table 6

Grouped Actor Categories

Grouped Category	Includes
Social Platforms	Social platforms, digital platforms, platform safety teams, platform users, UX designers, browser/app developers
Education Sector	Educators, students, education ministries, school administrators, educational institutions, libraries
Government & Regulators	Government, government agencies, policymakers, legislators, regulatory bodies, courts
Civil Society & NGO's	Civil society, NGO's (including international, journalism specific and fact-checking specific), community health clinics, human rights organizations
Tech Industry & Developers	AI developers, AI companies, authentication companies, cryptographic developers, cybersecurity firms, tech companies, digital ID providers
Academia & Experts	Academics, researchers, standards bodies, non-partisan experts, ethicists, legal scholars, professional associations
Media & News	News organizations, media outlets, public broadcasters, newsroom teams
International Bodies	UN, EU, G7/G20, multi-national tech forums

9.2.4. Estimated Timelines

In the context of the associated recommendations, the terms *short-term, medium-term*, and *long-term* are used to suggest general timeframes for implementing recommendations over the 5–10-year outlook. These categories are not predictive or fixed but are offered as guiding markers that reflect different levels of technical readiness, social complexity, and/or institutional inertia.

Short-term (0–2 years) includes actions that may be initiated immediately or in the very near future, typically those that build on existing tools or structures.

Medium-term (3–5 years) refers to efforts that may take several years to develop, scale, or coordinate. These actions tend to require more structured planning, developing technologies and policy support.

Long-term (5–10+ years) encompasses more complex or ambitious initiatives. These often face significant inertia, whether due to low technological maturity, entrenched behaviors or institutional lag.

These distinctions are intended to support planning rather than prescribe rigid timelines. They acknowledge that implementation will depend on a wide range of context/sector specific conditions and unpredictable factors.

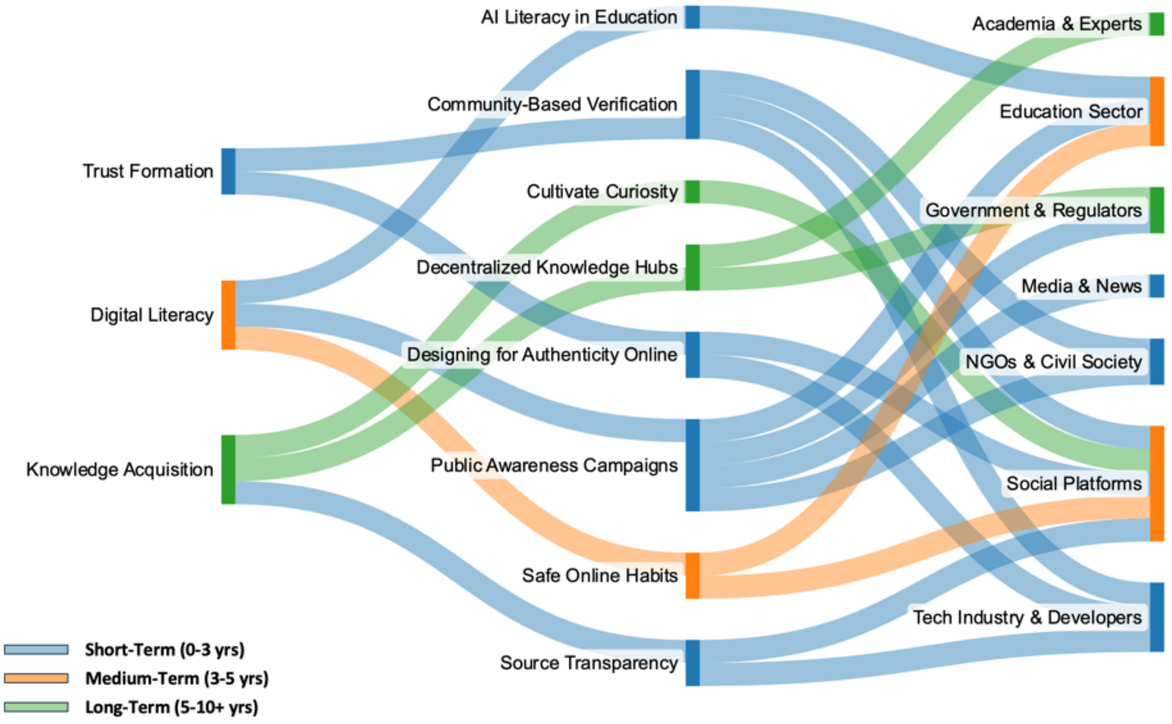
For a more detailed analysis of these timelines please refer to ***Appendix I***

9.3. Microsystem

The recommendations at this level focus on strengthening individual capacity for discernment, digital resilience, and epistemic agency. They prioritize practices for building trust, as well as critical and emotional literacy as tools to empower users to navigate growingly synthetic content and users more safely.

Figure 26

Microsystem-Level Recommendations Sankey Diagram



Note: This diagram maps Microsystem domains to targeted recommendations and relevant actor groups. Flows are color-coded by timeline: blue (short-term), orange (medium-term), and green (long-term).

9.3.1. Trust Formation

Community-Based Verification: Encourage the formation of local and online communities dedicated to collaboratively fact-checking information and flagging synthetic content. By involving people in verifying what they see and hear, interpersonal trust can be rebuilt through shared verification rather than leaving individuals isolated in doubt. This grassroots approach aims to counter the growing threat of what Ovadya (2018) terms “reality apathy,” the nihilistic distrust that arises when people suspect everything could be fake.

Actors: Social platforms, authentication companies, UX designers, civil society members, online communities. **Estimated Timeline**: Short-term.

Designing for Authenticity Online: Online platforms should move towards redesigning identity and interaction systems to emphasize *verified human presence*. Features such as visible indicators when content is AI-generated or when an account is verified human (and conversely warnings for likely bots) may help user more safely navigate platforms and their content. This approach aims to foster an online culture where genuine human voices are privileged in discourse, aiming to slowly rebuild trust in the information ecosystem before it collapses into cynicism. Platform policies might, for instance, down-rank content from unverified or bot-like accounts while highlighting posts from confirmed peoples. Simple design changes (such as a badge for "verified human" content creators or an authenticity score on profiles) can empower users to ensure they are interacting with real people, not synthetic personas.

Actors: Social platforms, UX designers, digital ID providers. **Estimated Timeline**: Short-term.

9.3.2. Digital Literacy

AI Literacy in Education: Make AI and synthetic media literacy a core component of curricula from K-12 through higher education. Students should learn how deepfakes, AI-generated text, and social bots are created, as well as how to critically evaluate digital content and sources. This equips the next generation to recognize manipulation and approach online information with healthy skepticism. In practice, this means teaching not just technical skills but also critical thinking habits (e.g. verifying sources before trusting or recognizing that virality does not guarantee truth). Educators and policymakers can collaborate to update lesson plans, train teachers and promote critical thinking at an early age.

Actors: Education ministries, school administrators, educators, students. **Estimated Timeline**: Short-term to implement, ongoing updates.

Public Awareness Campaigns: Launch widespread media and digital literacy campaigns for the general public, ensuring adults are not left behind by the rapid advance of emergent technologies. Community centers, libraries, and workplaces can host workshops on spotting misinformation and bots, while public broadcasters and social media can run informative content as they have for all sorts of health-related campaigns, ranging from smoking to drinking and driving. In a *"Digital Relief"* scenario, one could imagine governments and NGO's deploying "infodemic response teams" to educate communities in the wake of major disinformation crises, similar to how health workers respond to disease outbreaks. Investing now in awareness and upskilling can bring about that relief before the worst case scenario happens.

Actors: Government agencies, NGO's, libraries, media outlets, tech platforms. **Estimated Timeline**: Short-term.

Safe Online Habits & Emotional Skepticism: Modern digital literacy must extend beyond information consumption to behavior and emotional awareness. People of all ages should learn "online hygiene" practices that protect them and others in an AI rich environment. This includes guarding one's privacy (since personal data can be weaponized for scams or deepfakes) and using privacy settings to limit what bots can learn about you, as well as being cautious about what content one shares with AI services. It also means practicing respectful skepticism in interactions: rather than immediately accusing a stranger of being a bot (which can create witch-hunts), calmly seek verification. A key part of this education is an emotional skepticism**,** that recognizes that trust is often won through our emotions, and malicious bots will exploit outrage, fear or validation to manipulate us. Ultimately, stronger digital literacy that encompasses technical skills, critical thinking, *and* emotional intelligence will strengthen each person's ability to maintain their grip on reality in the face of digital manipulation.

Actors: Individual users, educators, browser/app developers; **Estimated Timeline**: Short-term to implement education, medium-term to adopt ongoing practices.

9.3.3. Knowledge Acquisition

Source Transparency in Search & AI Tools: Revamp search engines, recommendation systems, and AI tools to clearly show where information comes from and how it was generated. Results should label whether content is from a verified source, AI-generated, or of unknown origin, and include citations or tags users can quickly assess. These systems should also provide a range of credible viewpoints, not just a single answer, so users are able to see both consensus and legitimate dissent. For example, displaying "Most scientists say X, but some say Y" alongside provenance information such as "Source: Edited 2 days ago" helps users judge credibility at a glance. Tools should also nudge verification and critical thinking by flagging uncertainty (e.g. "This claim is unverified, here are two alternative views"). Designing with transparency and pluralism in mind aims to strengthens users' trust and makes our knowledge ecosystem more resilient to distortion.

Actors: Search engine companies, social platforms, AI developers, UX researchers; **Estimated Timeline**: Short-term.

Decentralized Knowledge Hubs: In the longer term, we may need to invest in knowledge infrastructures that are decentralized, and as such, less susceptible to manipulation and centralized oversight. This may look like an ecosystem of libraries, open-source archives and community-compiled knowledge systems that provide trustworthy information without centralized oversight. This means funding public repositories and collaborative projects (such as Wikipedia, open-source science efforts, digital libraries or the previously mentioned Metaweb) to ensure there are still verifiable sources and systems to consult in the digital world. We must endeavour to build new institutions or strengthen existing ones, so that people have some form of an anchor of truth even in this growing era of disinformation.

Actors: Policymakers, academics, open-source communities, technologists. **Estimated Timeline**: Long-term.

Cultivate Curiosity & Skepticism: Protecting our capacity to acquire reliable knowledge in the synthetic age requires cultivating a culture of curiosity paired with skepticism. Rather than passive consumers, individuals should be encouraged to become active investigators and participate in reporting false or suspicious claims. When many people take up the role of this investigator, the impact of misinformation is blunted, as false information is more quickly discovered. Platforms may also promote this behavior by rewarding users who help report and remove fake content, similar to how gaming platforms offer digital rewards for flagging cheaters or harassment.

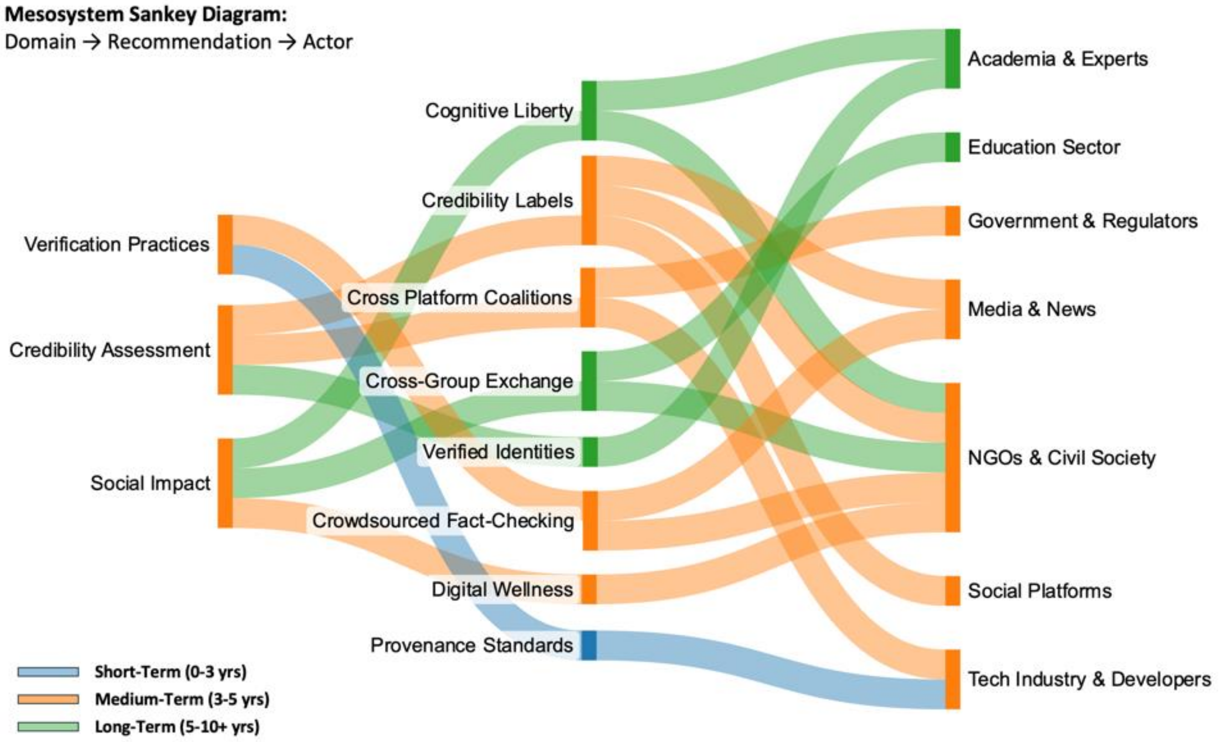
Actors: Digital platforms, platform users. **Estimated Timeline**: Long-term.

9.4. Mesosystem

The recommendations outlined at the Mesosystem level respond to the challenges of credibility, verification, and social impact that emerge between both offline and online communities. This level encompasses interactions across platforms, social networks, institutions, and content ecosystems. The recommendations in this category focus on developing shared standards, collaborative verification practices, and diverse credibility frameworks in order to try to mend fragmented trust and strengthen public discourse.

Figure 27

Mesosystem-Level Recommendations Sankey Diagram



Note: This diagram maps Mesosystem domains to targeted recommendations and relevant actor groups. Flows are color-coded by timeline: blue (short-term), orange (medium-term), and green (long-term).

9.4.1. Verification Practices

Provenance & Watermark Standards: Develop and widely adopt technical standards to trace the origins of content and watermark AI-generated media. This means creating machine-readable markers that indicate when an image, video, or audio has been AI generated or altered. Industry and standards bodies should collaborate on a common approach (some efforts like C2PA are already underway) so that any credible platform or device can automatically check for these markers. Over time, an expectation could emerge that unverified content must be met with healthy caution.

Actors: Technological standards bodies, Big Tech, cryptography experts, AI developers; **Estimated Timeline**: Short-term.

Crowdsourced Fact-Checking: Expand and support networks of fact-checkers and volunteers who can investigate viral content in real time. Recent experiments such as X's (Twitter's) Community Notes show that distributed communities can add context to claims quickly at scale. We should build on these models to create an agile verification layer across different platforms and systems. These responders would need tools (some of them AI-powered) to dissect content and track its spread, as well as legal and platform support to act swiftly without fear of liability when flagging falsehoods. While crowdsourced verification can't catch everything, its aim is to shorten the window of damage for misinformation.

Actors: Fact-checking NGO's, newsrooms, platform integrity teams. **Estimated Timeline**: Medium-term.

9.4.2. Credibility Assessment

Standard Credibility Labels: Develop a common set of credibility markers that news outlets, social platforms, and content creators can use to signal the trustworthiness of information at a glance. For example, an icon system or badges could denote: "Verified Publisher," "Fact-Checked," "AI-Generated (Labeled)," or "Source Identified." A rigorously checked report might display a green checkmark for having passed certain editorial standards, whereas a new blog post from an unknown source might show a grey warning icon until its information is corroborated. Implementing this consistently requires industry cooperation between major news organizations, tech platforms, and perhaps independent certification bodies agreeing on the definitions and design of these indicators.

Actors: News organizations, social platforms, developers, UX/UI designers, journalism NGO's. **Estimated Timeline**: Medium-term.

Cross Platform Coalitions: Misinformation and bot campaigns often spread across multiple platforms and communities. To counter this, a coalition among major social media companies, messaging apps, and search providers to share data and threat intelligence in real time may aid in preventing this spread. Similarly, if a network of bot accounts or a malicious troll farms is uncovered on one platform, that information (e.g. account handles, signatures of behavior) can be pooled in a common database accessible via API's to other platforms and to cybersecurity teams. Tech companies are already collaborating to some extent on removing terrorist propaganda and child sexual abuse material by sharing hashes of illegal content, and this same incentive may be extended to harmful or deceptive bot content.

Actors: Major tech companies, regulatory bodies, developers. **Estimated Timeline**: Medium-term.

Verified Identities & Expertise: Implement more robust verification of who is behind content. Journalists, officials, and experts could have verified digital signatures on their posts or articles, so readers know it's genuinely from them (and unaltered). Likewise, content from long-term verified human accounts could be visually distinguished from content by throwaway/ anonymous accounts. Over time, a reputation system can emerge as content from reputable identities are given more *initial* trust, whereas new or anonymous sources must *earn* trust through consistency or be subject to additional scrutiny. However, this recommendation needs careful balance to avoid creating a knowledge hierarchies. This ultimately aims to make it harder for bots to impersonate trusted figures or for false personas to gain large followings.

Actors: Platform policy teams, identity verification services, professional associations. **Estimated Timeline**: Long-term.

9.4.3. Social Impact

Digital Wellness & Mental Health: Living amid constant misinformation and uncertain reality takes a psychological toll, including anxiety, mistrust, and even radicalization or despair. A holistic response to the explosion of emergent technologies should therefore include tending to people's mental and emotional well-being by recognizing the harms caused by these rapidly evolving technologies. Therefore, we should endeavour to provide resources such as counseling, support groups, or workshops for those overwhelmed or affected by digital harms.

Actors: Mental health professionals, public health departments, community health clinics. **Estimated Timeline**: Medium-term to research and implement good practices.

Cross-Group Exchange: Actively aim to bring different demographics or ideological groups together to examine media and issues in a constructive setting. For instance, host dialogues between different political party voters to jointly review a controversial news story with a fact-checker mediating. These cross community interactions can also be implemented in educational settings as thought exercises, in order to encourage breaking down echo chambers and building resilience against divisive propaganda by humanizing the "other" and finding common grounds.

Actors: NGOs, educational institutions, interfaith groups, city councils. **Estimated Timeline**: Long-term.

Protect Cognitive Liberty: Treat freedom of thought as a right under threat. Encourage policies and norms that condemn extreme manipulative practices (like deepfake smear campaigns or hyper-targeted psy-ops) as violations of people's cognitive autonomy. This principle can guide regulations similar to how we protect privacy and free speech, in order to safeguard the integrity of individual thought against AI enabled distortion

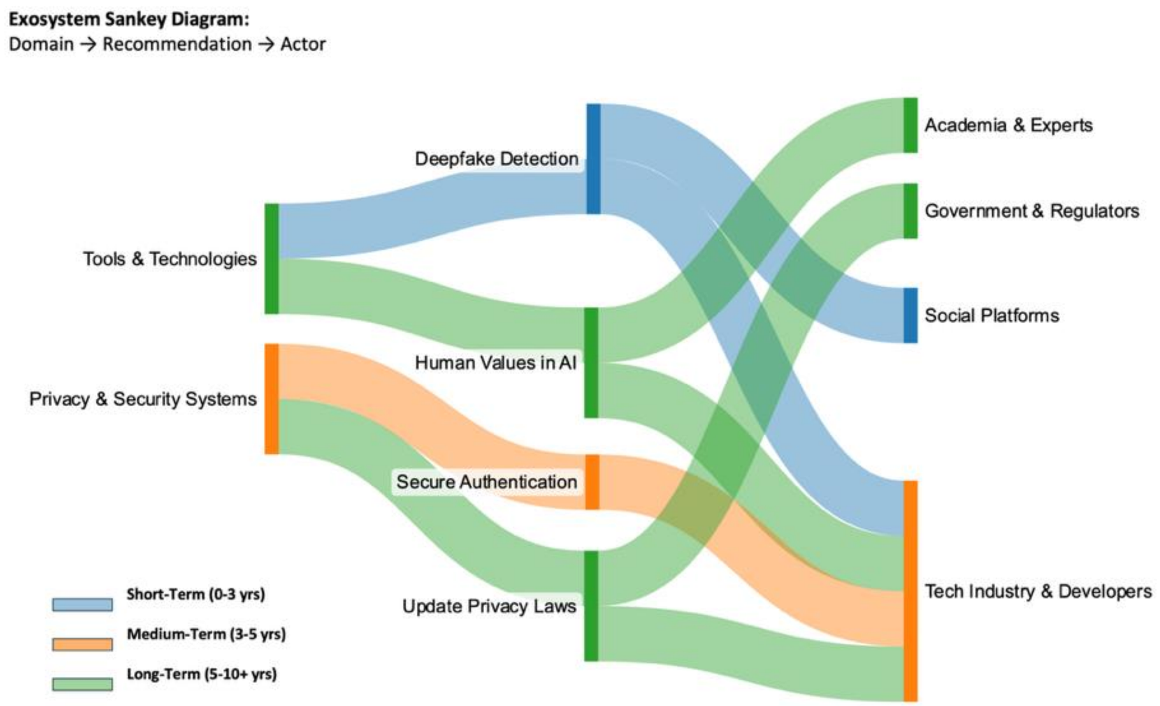
Actors: human rights organizations, ethicists, lawmakers. **Estimated Timeline**: Long-term**,** integrated into legal frameworks.

9.5. Exosystem

The recommendations developed at the Exosystem level focus on the building and design of more trustworthy technical systems including more robust and accessible detection tools, as well as privacy protections to ensure that our digital ecosystems remain navigable, equitable, and defensible against cyber threats.

Figure 28

Exosystem-Level Recommendations Sankey Diagram



Note: This diagram maps Exosystem domains to targeted recommendations and relevant actor groups. Flows are color-coded by timeline: blue (short-term), orange (medium-term), and green (long-term).

9.5.1. Tools & Technologies

AI Deepfake Detection & Monitoring: A suite of Digital Content Authentication Technologies (DCAT) (Cooke, 2025) should be implemented widely. This involves an arsenal of detective algorithms watching out for fakes in real time. These include AI models trained to recognize artifacts or patterns left by generative models in images and audio, algorithms that analyze writing style or metadata to catch AI-written text, and network analysis tools that spot bot activity on social networks. Major platforms can integrate such detectors on their servers and browsers can offer extensions that locally warn users about content. To stay effective, these detection AI’s need constant updating, as synthetic media grows more sophisticated. Therefore they will require sustained investment in R&D, perhaps aided by national or global incentives as well as collaborative databases of known deepfakes that detectors can train on.

Actors: AI research labs, cybersecurity firms, platform safety teams, government R&D funding. **Estimated Timeline**: Short-term to deploy current technological capabilities, continuous updates as technologies advance).

Human Values in AI Design: Shift AI development to embed human values, oversight, and agency into the design of its systems. Rather than reacting to harms after AI is deployed, we must anticipate and prevent those harms by setting guardrails in how we build these systems. Concretely, developers can implement stricter guidelines in their models making it technically easier to detect if a piece of content has been AI generated. They can also include user controls and transparency by default; such as AI that always provides citations with dates of retrieval for its outputs. Legal and regulatory frameworks should encourage this proactive stance. For example, regulators might require that any AI capable of generating audio of a person's voice must include a watermarking feature.

Actors: AI companies, regulators, ethicists, standards bodies. **Estimated Timeline**: Short-term piloting voluntary or broad regulatory guidelines, Long-term to bake in industry norms/regulations and user awareness.

9.5.2. Privacy & Security Systems

Update Data Privacy Laws: Strengthen privacy laws and practices to limit how much or what type of personal data can be collected or sold without consent, in order to prevent ongoing security risks. For example, enforce stricter penalties for companies that leak data, including audio and video files, and continue to encourage features such as end-to-end encryption. By protecting personal data, we make it harder for attackers to engage in fraud and the ability to craft effective personalized fakes.

Actors: Legislators, data protection agencies, tech companies, privacy advocates. **Estimated Timeline**: Long-term legislative changes, with incremental improvements sooner.

Secure Authentication of Information: Upgrade the technical infrastructure that verifies sources and content. Implement measures such as: widespread use of digitally signed emails and documents, verified logos on genuine communications (e.g. banks & governments have a cryptographic seal in emails known as the BIMI standard), and content signing for media (every news video has a publisher signature). This way, if a fake piece of content circulates, devices and apps can automatically tell it lacks a valid signature or has been tampered with. We can also strengthen key platforms against impersonation by offering an encrypted verification stamp for official pages, and browsers can warn if a site is not presenting expected credentials. All these means make it more difficult for fakes to pose as real entities by hijacking known channels.

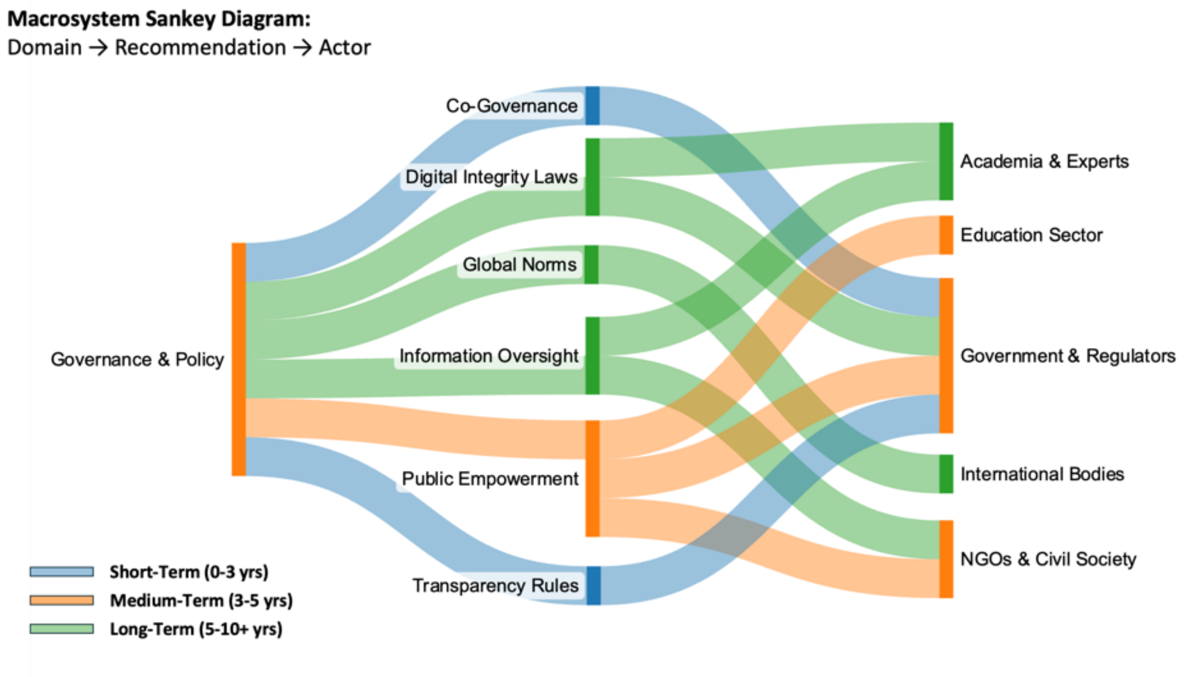
Actors: Cryptographic developers, cybersecurity standards bodies, major tech providers.
Estimated Timeline: Medium-term to implement known solutions, Long-term for wide adoption.

9.6. Macrosystem

The recommendations at this level focus on establishing transparency mandates, global norms, independent oversight, and co-governance structures capable of sustaining the integrity of digital life across borders and generations.

Figure 29

Macrosystem-Level Recommendations Sankey Diagram



Note: This diagram maps Macrosystem domain of Governance & Policy to targeted recommendations and relevant actor groups. Flows are color-coded by timeline: blue (short-term), orange (medium-term), and green (long-term).

9.6.1. Governance & Policy

Transparency & Disclosure Rules: Enact policies that require clear labeling of synthetic content and algorithmic transparency. This may look like deepfakes, synthetic entities or AI-modified videos being tagged as such (with legal penalties for deliberate omission), requiring platforms to publicly report the scale of bot activity and mandating they pursue ongoing measures to mitigate said spread. Mandate third-party audits for content recommendation systems, in which companies provide regulators or researchers access to analyze how their algorithms might be spreading false or harmful content. These measures push both creators of content and platforms to be accountable for curbing harmful synthetic media.

Actors: Legislators, regulatory agencies, digital platform companies. **Estimated Timeline**: Short-term for drafting key rules, Medium-term for enforcement.

Public Awareness & Empowerment Campaigns: Governments should fund and support initiatives that educate and empower the public. This includes grants for media literacy programs in schools, public service campaigns about deepfake/synthetic manipulation awareness, and community workshops via libraries or programs. In emergencies, authorities may set up an official verified information feed or hotline to counter widespread rumors so that citizens may at least be able to receive some consensus from their governments as to emergent crises. Investing in these initiatives makes society less likely to fall for or spread fakes, complementing the efforts to stop the fakes at the source and possibly reinforcing trust in larger institutions simultaneously.

Actors: Government (public education, communication departments), NGOs, Educational institutions. **Estimated Timeline**: Short to medium-term to create policy, allocate funding, & commit to ongoing execution.

Global Norms and Cooperation: Continue to work internationally to agree on norms and joint actions regarding creation of synthetic media and entity misuse. For example, pursue an international agreement that countries will not use deepfakes for propaganda or will cooperate in tracing cross-border disinformation campaigns with possibility of legal recourse. Form international rapid alert networks for new misinformation tactics (similar to countries sharing cyber threat intelligence). Potentially treat malicious deepfake attacks by state or proxy actors as a "hostile act" subject to sanctions or other responses. A global approach helps close safe havens for bad actors and sets expectations that manipulating digital ecosystems, and the havoc it reigns on society, is a recognized global threat

Actors: UN, EU, G7/G20, international NGOs, multi-national tech forums. **Estimated Timeline**: Medium-term to negotiate charters, Long-term to establish enforcement.

Co-Governance Structures: Establish multi-stakeholder bodies (mix of government, industry, academia & civil society) that continuously address AI and information integrity issues. These could operate as ongoing task forces that regularly evaluate emerging threats and recommend mitigative actions. By having all stakeholders at the table and iterating quickly, this approach keeps governance responsive and up-to-date with fast-evolving technology

Actors: Policymakers, major tech firms, universities, journalism and civil rights NGO's, user representatives. **Estimated Timeline**: Short-term to create initial councils, medium-term to apply adjudications.

Laws Protecting Digital Integrity: Update legal frameworks to penalize malicious uses of synthetic entities/media and affirm the importance of truthful information. Make certain uses of deepfakes explicitly illegal (e.g. fake videos to incite violence or fraud). Enhance legal recourse for victims of deepfake defamation or impersonation (simplify takedown and lawsuit processes). Consider recognizing “cognitive security” or freedom from deceptive manipulation as a protected value in law, which could guide future regulations and court rulings. Encourage development of standards, or even treaties, that treat large scale disinformation campaigns as illegal (similar to bans on cyber-attacks or biological weapons). The law should also push transparency, requiring platforms to feature provenance systems to allow for users to track its content source. While balancing freedom of expression, these legal moves draw a clear line that deliberately eroding the shared sense of reality (through known falsehoods, impersonation, fake evidence, etc.) is a serious wrongdoing. It provides a backstop so even as technology evolves, the most harmful conduct is constrained by law.

Actors: National legislatures, technological regulatory bodies, courts, legal scholars. **Estimated Timeline**: Long-term (with incremental statutes coming earlier).

Digital Information Oversight Body: Create an independent body focused on monitoring and ensuring the integrity of information ecosystems. Functions might include tracking levels of misinformation (an index or regular report), auditing big platforms’ compliance with transparency and anti-bot measures, coordinating cross-sector responses to major incidents (like a deepfake crisis), and advising on new policies. This agency would ideally be non-partisan and staffed by experts in tech, media, and social science. It could operate somewhat like a central bank (but for information) or a public knowledge utility. The existence of a dedicated organization would ensure continuous attention to the issue, not just reactive, and a holistic approach that isn’t tied to one platform or election cycle. Over time, it could become a trusted referee for sustaining a sense of a shared reality (e.g. debunking or confirming contested content neutrally)

Actors: International and national regulatory bodies, academia, civil society, non-partisan experts. **Estimated Timeline**: Long-term to build, as it requires political consensus and public trust.

9.7. Remarks on Recommendations

The series of recommendations outlined in the previous section, while thorough, are inherently partial measures. They reflect an exploratory approach to a complex set of challenges rather than an exhaustive solution. In practice, these ideas aim to support further learning and adaptation, not definitive endpoints. They are offered with humility, aware that no single strategy can resolve the issue in full but recognize that these steps provide a constructive starting point.

For all their promise, even the best interventions leave open a core tension: We have not *eliminated* the fundamental question of how to sustain shared and private realities under these growing synthetic conditions. How can we begin to engage with these dilemmas, let alone act on the recommendations without a shared consensus on reality, or even reliable access to our own? Acknowledging this gap is not a concession of defeat, but rather a recognition of the deeper stakes at hand. It reminds us that our challenge is as existential as it is technical.

10. Conclusion

This research began with a question that, though once considered speculative or conspiratorial, has taken on renewed urgency in light of emerging realities: *How might widespread synthetic content and bot activity reshape human experiences and interactions, both online and off, over the next 5 to 10 years?*

To investigate this, the study employed a neo-ecological systems framework, an evolution of Bronfenbrenner's ecological model, that explicitly integrates the virtual alongside the physical. This framework enabled structuring challenges and insights across interrelated domains: from the individual and interpersonal dynamics of the micro- and meso- systems, through to the institutional and governance layers stretching to the macrosystem. Utilizing a State-of-the-Art literature review, expert interviews, and a reflexive thematic analysis, the research surfaced significant patterns, key tensions and emergent trends introduced by the proliferation of bots, synthetic content, and emergent technologies.

The findings from this research presented a layered understanding of the disruptions both developing and at hand. At the microsystem level, synthetic content was found to challenge foundational processes of trust formation, digital literacy, and knowledge acquisition, effectively distorting not just what we know, but how we come to know it. The mesosystem revealed breakdowns in credibility assessment and verification practices, raising concerns about how individuals navigate and evaluate information within digital and physical environments. The exosystem exposed increasing vulnerability in the tools and infrastructures intended to safeguard user experience, while the macrosystem highlighted the ongoing regulatory asymmetries and geopolitical complexities that inhibit coordinated responses.

To extend the analysis beyond current trajectories, the research engaged in a strategic foresight inquiry. Ten change drivers were identified and organized through a STEEP+V lens, highlighting the forces most likely to disrupt or transform the systems in question. A 2x2 scenario matrix was developed, structured around the critical uncertainties of *Digital Verification Capability* and *Societal Trust Patterns*. These four worlds: *Pay for Trust*, *Digital Relief*, *Dark Forests vs The Public Internet*, and *The Community Web*, served not as predictions but as plausible futures through which to examine diverging outcomes and determine recommendations. The scenarios illuminated both the potential risks of systemic breakdowns, and the potential for more cooperative configurations across our physical and digital lives; illuminating how evolving trends may give rise to wildly different consequences.

From these insights emerged a set of recommendations, organized across the neo-ecological levels and mapped to estimated timelines and actors. These recommendations, ranging from provenance standards and co-governance structures to public awareness campaigns and credibility tools, reinforce the position that addressing these challenges requires coordinated responses across a breadth of actors; each supporting the other to create the conditions necessary for us to thrive (not just survive).

The question of synthetic presence is no longer about *if*, but *how*. These technologies are not peripheral, they are becoming infrastructural. Our task ahead lies in our willingness and ability (amidst a landscape of growing power asymmetries) to shape them toward public interest goals and shared epistemic resilience. If digital environments are now entangled with the very systems by which we interpret and engage with the world, then the responsibility may fall on us to ensure that they *enable* and not *erode* the foundations of what makes us human.

11. Coda

The Future of our Realities

"Authenticity is de facto dead"; the real self may be diminished: Humans have to adapt to the multiplicity of the self and more one-way relationships and isolation due to personalized "realities" that could lead to the fragmentation of one's core sense of identity" - Tracey Follows, CEO of Futuremade, a leading UK-based strategic consultancy (as cited in Anderson & Rainie, 2025, p. 44)

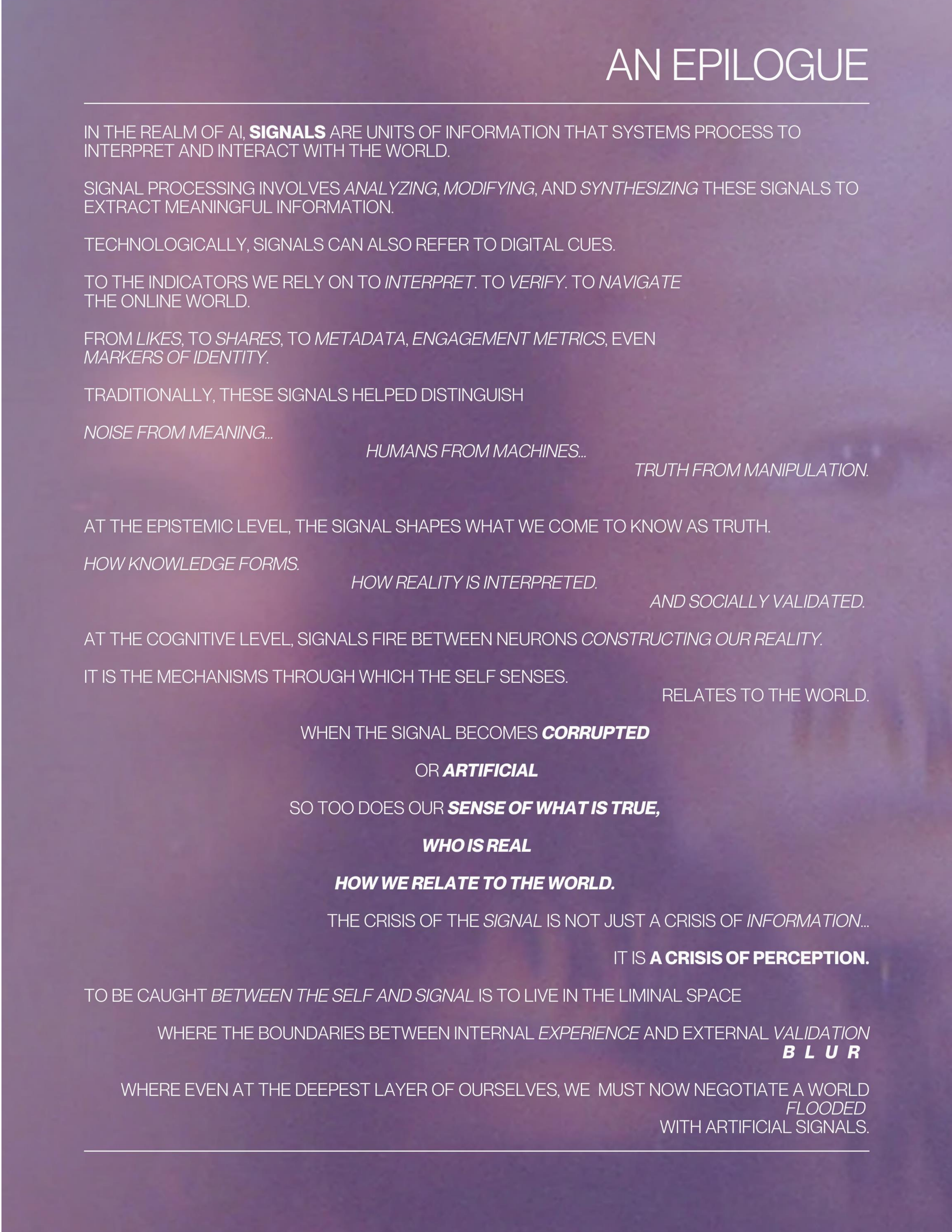
The evolutionary trajectory of the Dead Internet Theory, from digital skepticism to existential challenge, suggests we may be entering uncharted territory in the human experience. When the mechanisms through which we establish our realities are systematically manipulated by synthetic actors, and when our physical environment becomes increasingly obfuscated, traditional anchors for reality determination erode in front of us.

Yet humans have proven remarkably adaptable throughout history. As our research identified, cyclical patterns in trust, in technological adaptation (even with over-automation of our phone help lines) have already occurred, and we have been able to bounce back time and time again. This suggests that rather than simple linear decline, new mechanisms and approaches will eventually emerge to mitigate these threats. The question remains whether these adaptations will occur rapidly enough to prevent significant social, psychological, and physical harm as these systems continue their exponential advance, or if AI will truly be the outlier to disrupt to these cycles.

The ultimate challenge may be preserving what we identify as our distinctively human capacity for connection, expression, and reality construction that exists beyond algorithmic prediction and synthetic manipulation. As Aviv Ovadya (2018) claims, this is a battle we must fight if we want to avert an Infopocalypse and maintain a functioning civilization. In navigating this challenge, we may discover not only new ways to distinguish the human from the non-human, but also a deeper understanding and appreciation of what makes the human experience *uniquely* valuable in an increasingly artificial world. How many of us just wanted to go to a concert? Sit in a busy café? Or receive a hug during the pandemic? How many of us are already sick of those uncanny, AI generated images?

These potential futures may well hinge on how we answer the fundamental query that emerges from this research: *How do we maintain a shared and private sense of reality when the very mechanisms we use to establish that reality, whether it be cognitive liberty, social verification, sensory perception, or even institutional authorities, are increasingly subject to systematic manipulation?* The answer will determine (and I recognize the heavy-handedness of this statement) not just the future of the internet, but the future trajectory of a human-centred society itself. As Echterhoff et al. (2009) note, the experience of having commonality with others' inner states, fulfills *not only our need for valid beliefs*, but also *our fundamental need for human connection*. A connection, that non-human systems, no matter how sophisticated, cannot genuinely replicate.

P.S. The Imperva Bad Bot report **2025** came out the week of this work's submission…
we passed 50% ... bots now account for a **majority of all internet activity**… stay safe.



AN EPILOGUE

IN THE REALM OF AI, **SIGNALS** ARE UNITS OF INFORMATION THAT SYSTEMS PROCESS TO INTERPRET AND INTERACT WITH THE WORLD.

SIGNAL PROCESSING INVOLVES *ANALYZING*, *MODIFYING*, AND *SYNTHESIZING* THESE SIGNALS TO EXTRACT MEANINGFUL INFORMATION.

TECHNOLOGICALLY, SIGNALS CAN ALSO REFER TO DIGITAL CUES.

TO THE INDICATORS WE RELY ON TO *INTERPRET*. TO *VERIFY*. TO *NAVIGATE*
THE ONLINE WORLD.

FROM *LIKES*, TO *SHARES*, TO *METADATA*, *ENGAGEMENT METRICS*, EVEN
MARKERS OF IDENTITY.

TRADITIONALLY, THESE SIGNALS HELPED DISTINGUISH

NOISE FROM MEANING...
HUMANS FROM MACHINES...
TRUTH FROM MANIPULATION.

AT THE EPISTEMIC LEVEL, THE SIGNAL SHAPES WHAT WE COME TO KNOW AS TRUTH.

HOW KNOWLEDGE FORMS.
HOW REALITY IS INTERPRETED.
AND SOCIALLY VALIDATED.

AT THE COGNITIVE LEVEL, SIGNALS FIRE BETWEEN NEURONS *CONSTRUCTING OUR REALITY.*

IT IS THE MECHANISMS THROUGH WHICH THE SELF SENSES.
RELATES TO THE WORLD.

WHEN THE SIGNAL BECOMES ***CORRUPTED***

OR ***ARTIFICIAL***

SO TOO DOES OUR ***SENSE OF WHAT IS TRUE,***

WHO IS REAL

HOW WE RELATE TO THE WORLD.

THE CRISIS OF THE *SIGNAL* IS NOT JUST A CRISIS OF *INFORMATION...*

IT IS **A CRISIS OF PERCEPTION.**

TO BE CAUGHT *BETWEEN THE SELF AND SIGNAL* IS TO LIVE IN THE LIMINAL SPACE

WHERE THE BOUNDARIES BETWEEN INTERNAL *EXPERIENCE* AND EXTERNAL *VALIDATION*
BLUR

WHERE EVEN AT THE DEEPEST LAYER OF OURSELVES, WE MUST NOW NEGOTIATE A WORLD
FLOODED
WITH ARTIFICIAL SIGNALS.

References

Achiam, O. J., Adler, S., Agarwal, S., Ahmad, L., Akkaya, I., Aleman, F. L., Almeida, D., Altenschmidt, J., Altman, S., Anadkat, S., Avila, R., Babuschkin, I., Balaji, S., Balcom, V., Baltescu, P., Bao, H., Bavarian, M., Belgum, J., Bello, I., ... Zoph, B. (2023). GPT-4 Technical Report. [Technical report].

Afroogh, S., Akbari, A., Malone, E., Kargar, M., & Alambeigi, H. (2024). Trust in AI: Progress, challenges, and future directions. *arXiv*. http://arxiv.org/abs/2403.14680

Alajmi, M., Elashry, I., El-sayed, H., & Faragallah, O. (2020). A password-based authentication system based on the CAPTCHA AI problem. *IEEE Access, 8*, 161703–161713. https://doi.org/10.1109/ACCESS.2020.3018659

Amer, M., Daim, T., & Jetter, A. (2013). A review of scenario planning. *Futures, 46*, 23-40. https://doi.org/10.1016/j.futures.2012.10.003

Anderson, J., & Rainie, L. (2025, April 2). *Expert views on the impact of AI on the essence of being human*. Imagining the Digital Future Center, Elon University. https://www.elon.edu/u/news/2025/04/02/report-technology-experts-worry-about-the-future-of-being-human-in-the-ai-age/

Angwin, J. (2024, December 9). The future of trustworthy information: Learning from online content creators. *Shorenstein Center*. https://shorensteincenter.org/future-trustworthy-information-learning-online-content-creators/

ANTICIPATE, Dakinah, K., Christine Hejselbæk, S., & Behn Bjørnhof, M. (2025, April). *Megatrends- 5. Blurring Realities*. ANTICIPATE. https://www.anticipate.dk/megatrends/blurring-realities

Appleton, M. (2023). *The Expanding Dark Forest and Generative AI*. Maggieappleton.com. https://maggieappleton.com/forest-talk/

Balagopalan, A., Madras, D., Yang, D. H., Hadfield-Menell, D., Hadfield, G. K., & Ghassemi, M. (2023). Judging facts, judging norms: Training machine learning models to judge humans requires a modified approach to labeling data. *Science Advances, 9*(19), eabq0701. https://doi.org/10.1126/sciadv.abq0701

Balagopalan, A., et al. (2023). Deepfakes and the crisis of digital authenticity. *Journal of Ethics in AI, 12*(3), 45–67.

Barry, E. S., Merkebu, J., & Varpio, L. (2022). Understanding state-of-the-art literature reviews. *Journal of Graduate Medical Education, 14*(6), 659-662. https://doi.org/10.4300/JGME-D-22-00705.1

Bawden, D. (2008). Origins and concepts of digital literacy. In C. Lankshear & M. Knobel (Eds.), *Digital literacies: Concepts, policies and practices* (pp. 17-32). Peter Lang Publishing.

Bennett, W. L., & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication, 33*(2), 122-139. https://doi.org/10.1177/0267323118760317

Blue, J., Condell, J., & Lunney, T. (2018). A review of identity, identification and authentication. *International Journal for Information Security Research, 8*(2), 794-804.

Blum, S. (2025, January 17). *Bluesky's Bot Problem Is a Byproduct of Its Success. Users Are Not Amused.* Inc. https://www.inc.com/sam-blum/blueskys-bot-problem-is-a-byproduct-of-its-success-users-are-not-amused/91108986

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2012). Thematic analysis. In H. Cooper, P. M. Camic, D. L. Long, A. T. Panter, D. Rindskopf, & K. J. Sher (Eds.), *APA handbook of research methods in psychology, Vol. 2: Research designs* (pp. 57–71). American Psychological Association.

Braun, V., & Clarke, V. (2020). One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative Research in Psychology, Advance online publication*. https://doi.org/10.1080/14780887.2020.1769238

Braun, V., & Clarke, V. (2014). Thematic analysis. In T. Teo (Ed.), *Encyclopedia of critical psychology* (pp. 1947–1952). Springer. https://doi.org/10.1007/978-1-4614-5583-7_311

Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health, 11*(4), 589–597. https://doi.org/10.1080/2159676X.2019.1628806

Bridgit DAO. (2023). The Metaweb: The Next Level of the Internet (1st ed.). CRC Press. https://doi.org/10.1201/9781003225102

Bridle, J. (2022, March 15). The dead internet and the ends of networked humanism. *MIT Technology Review*. https://www.technologyreview.com/2022/03/15/1047304/dead-internet-networked-humanism/

Brin, S., & Page, L. (1998). The anatomy of a large-scale hypertextual web search engine. *Computer Networks and ISDN Systems, 30*(1-7), 107-117.

Bron, D. (2023, October 6). Artificial minds, genuine bonds: The role of AI in shaping future human relationships. *Chain Reaction*. https://medium.com/chain-reaction/artificial-minds-genuine-bonds-the-role-of-ai-in-shaping-future-human-relationships-in-the-2e73d8d9e7ec

Bronfenbrenner, U. (1979). *The Ecology of Human Development: Experiments by Nature and Design*. Harvard University Press. https://doi.org/10.2307/j.ctv26071r6

Byrne, D. (2021). A worked example of Braun and Clarke's approach to reflexive thematic analysis. *Quality & Quantity, 56*(3), 1391-1412. https://doi.org/10.1007/s11135-021-01182-y

Citron, D. K., & Chesney, R. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*, 1753. https://scholarship.law.bu.edu/faculty_scholarship/640

Cole, E. (2013). *Advanced persistent threat: Understanding the danger and how to protect your organization*. Syngress.

Collet, V., & Ciminelli, M. (2017). Polyphonic analysis: Obuchenie in qualitative research. *Qualitative Research Journal, 17*, 00-00. https://doi.org/10.1108/QRJ-08-2016-0053

Confessore, N. (2018). Cambridge Analytica and Facebook: the Scandal and the Fallout so Far. *The New York Times*. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Constantin, L. (2024, October 3). *DDoS attacks are increasingly targeting critical infrastructure*. CSO Online. https://www.csoonline.com/article/3545049/ddos-attacks-are-increasingly-targeting-critical-infrastructure.html

Cooke, D. (2025, January 17). *Building a Digital Content Authentication Research Ecosystem*. Federation of American Scientists. https://fas.org/publication/digital-content-authentication-ecosystem/

Cooke, E., Jahanian, F., & McPherson, D. (2005, July). *The zombie roundup: Understanding, detecting, and disrupting botnets*. In *Proceedings of the 2005 USENIX Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI '05)* (pp. 39–44). USENIX Association. https://www.usenix.org/legacy/event/sruti05/tech/full_papers/cooke/cooke.pdf

Copyleaks. (2024, April 30). Copyleaks analysis reveals explosive growth of AI content across the web. https://copyleaks.com/about-us/press-releases/copyleaks-analysis-reveals-explosive-growth-of-ai-content-across-the-web

CP2A. (2024). *Guiding Principles - C2PA*. C2pa.org. https://c2pa.org/principles/

DataDome. (2022, November 5). What's the difference between good bots and bad bots? https://datadome.co/guides/bot-protection/good-bots-vs-bad-bots-and-when-you-should-block-them/

Davis, C. A., Varol, O., Ferrara, E., Flammini, A., & Menczer, F. (2016). Botometer: A system to detect social media bots. *Proceedings of the 10th International AAAI Conference on Web and Social Media*, 273-274.

Denardis, L. (2014). *The Global War for Internet Governance*. Yale University Press. https://doi.org/10.2307/j.ctt5vkz4n

DeIuliis, D. (2015). Gatekeeping theory from social fields to social networks. *Communication Research Trends, 34*(1), Article 1. https://scholarcommons.scu.edu/crt/vol34/iss1/1

Diepeveen, S. (2024, January 18). *Has AI ushered in an existential crisis of trust in democracy?* ODI Global. https://odi.org/en/insights/has-ai-ushered-in-an-existential-crisis-of-trust-in-democracy/

Ding, X., Carik, B., Gunturi, U. S., Reyna, V., & Rho, E. H. (2024). Leveraging prompt-based large language models: Predicting pandemic health decisions and outcomes through social media language. *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 1-20. https://doi.org/10.1145/3613904.3642117

Echterhoff, G., Higgins, E. T., & Levine, J. M. (2009). Shared Reality: Experiencing Commonality With Others' Inner States About the World. *Perspectives on psychological* *science : a journal of the Association for Psychological Science*, *4*(5), 496–521. https://doi.org/10.1111/j.1745-6924.2009.01161.x

Edelman Trust Barometer. (2024). *Global Report*. Edelman Trust Institute. https://www.edelman.com/sites/g/files/aatuss191/files/2024-02/2024%20Edelman%20Trust%20Barometer%20Global%20Report_FINAL.pdf

Edwards, B. (2022, September 16). Twitter pranksters derail GPT-3 bot with newly discovered "prompt injection" hack. *Ars Technica*. https://arstechnica.com/information-technology/2022/09/twitter-pranksters-derail-gpt-3-bot-with-newly-discovered-prompt-injection-hack/

European Union. (2023). EU AI Act. https://digital-strategy.ec.europa.eu/en/library/eu-ai-act

Eysenbach, G. (2008). Credibility of health information and digital media: New perspective and implications for youth. In M. J. Metzger & A. J. Flanagin (Eds.), *Digital media, youth, and credibility* (pp. 123-154). MIT Press.

Farrier, D. (2024, March 19). *Why Is Facebook Just Shrimp Jesus?* Webworm.co; Webworm with David Farrier. https://www.webworm.co/p/why-is-facebook-just-shrimp-jesus

Federal Bureau of Investigation. (2010, October 1). Cyber bust. https://archives.fbi.gov/archives/news/stories/2010/october/cyber-banking-fraud

Feldman, S. (2019, October 30). *What is the state of digital literacy in the USA?* World Economic Forum. https://www.weforum.org/stories/2019/10/americans-get-a-failing-grade-for-digital-literacy/

Ferrara, E. (2019). *Bots, elections, and social media: A brief overview* [Preprint]. arXiv. https://arxiv.org/abs/1910.01720

Ferrara, E. (2023). Social bot detection in the age of ChatGPT: Challenges and opportunities. *First Monday, 28*(6). https://doi.org/10.5210/fm.v28i6.13185

Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. *Communications of the ACM*, *59*(7), 96–104. https://doi.org/10.1145/2818717

Floridi, L. (2023). The ethics of generative AI: A framework for accountability. *Philosophy & Technology, 36*(1), 1-22.

Fogg, B. J. (2002). Persuasive technology: Using computers to change what we think and do. *Ubiquity, 3*. https://doi.org/10.1145/763955.763957

Gillies, B. (2024, March 28). 4 Canadian school boards sue Snapchat, TikTok and Meta for disrupting students' education. *AP News*. https://apnews.com/article/canada-schools-social-media-lawsuit-179873076587ca57ba7e24f836dc604b

Gobika, S., & Vaishnavi, N. (2025). Blockchain based identity management system. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11*, 1413-1420. https://doi.org/10.32628/CSEIT25112471

Godet, M. (2000). The art of scenarios and strategic planning: Tools and pitfalls. *Technological Forecasting and Social Change, 65*(1), 3–22. https://doi.org/10.1016/S0040-1625(99)00120-1

Goh, B. (2018, August 29). China police investigate possible data breach at hotel operator Huazhu. *Reuters*. https://www.reuters.com/article/technology/china-police-investigate-possible-data-breach-at-hotel-operator-huazhu-idUSKCN1LE0GC/

Google. (n.d.). *Choosing the type of reCAPTCHA*. Google Developers. Retrieved April 13, 2025, from https://developers.google.com/recaptcha/docs/versions

Gray, M. (1996, June 20). *Internet Growth and Statistics: Credits and Background*. Mit.edu; Massachusetts Institute of Technology. https://www.mit.edu/~mkgray/net/background.html

Gunadi, R. A. A., & Lubis, M. (2023, May). The effect of digital literacy on children violence. In *1st UMSurabaya Multidisciplinary International Conference 2021 (MICon 2021)* (pp. 700-706). Atlantis Press.

Guy-Evans, O. (2024). Bronfenbrenner's Ecological Systems Theory [Online Image]. In *simplypsychology.org*. https://www.simplypsychology.org/bronfenbrenner.html

Haleem, A., Javaid, M., Qadri, M. A., Singh, R. P., & Suman, R. (2022). Artificial intelligence (AI) applications for marketing: A literature-based study. *International Journal of Intelligent Networks, 3*, 119–132. https://doi.org/10.1016/j.ijin.2022.08.005

Harris, Keith Raymond (2023). Liars and Trolls and Bots Online: The Problem of Fake Persons. Philosophy and Technology 36 (2):1-19.

Hern, A. (2024, April 30). TechScape: On the internet, where does the line between person end and bot begin? *The Guardian*. https://www.theguardian.com/technology/2024/apr/30/techscape-artificial-intelligence-bots-dead-internet-theory

Hiltunen, E. (2009). Scenarios: Process and outcome. *Journal of Futures Studies, 13*(3), 151-152.

Hogg, M. A., & Rinella, M. J. (2018). Social identities and shared realities. *Current Opinion in Psychology, 23*, 6–10. https://doi.org/10.1016/j.copsyc.2017.10.003

Holdsworth, J., & Kosinski, M. (2024, July 26). *Information Security*. Ibm.com; IBM (International Business Machines Corporation). https://www.ibm.com/think/topics/information-security

Huang, Y. (2024, December 4). Deepfake fraud: How AI is bypassing biometric security in financial institutions. https://www.group-ib.com/blog/deepfake-fraud

IBM. (2023, May 12). *What is the Internet of Things (IoT)?* IBM. https://www.ibm.com/think/topics/internet-of-things

IEEE. (2023). Ethically aligned design: A vision for prioritizing human well-being with autonomous and intelligent systems. https://standards.ieee.org/wp-content/uploads/import/documents/other/ead_v2.pdf

IlluminatiPirate. (2021, January 5). Dead internet theory: Most of the internet is fake. *Agora Road's Macintosh Cafe*. https://forum.agoraroad.com/index.php?threads/dead-internet-theory-most-of-the-internet-is-fake.3011/

Imperva. (2023). Bad bot report 2023. https://www.imperva.com/resources/resource-library/reports/bad-bot-report-2023/

Imperva. (2024a). Bad bots report 2024. Imperva Research Labs. https://www.imperva.com/resources/resource-library/reports/2024-bad-bot-report/

Imperva. (2024b, September 18). Vulnerable APIs and bot attacks costing businesses up to $186 billion annually. https://www.imperva.com/company/press_releases/vulnerable-apis-and-bot-attacks-costing-businesses-up-to-186b-annually/

International Institute for Management Development (IMD). (2022, November 2). Everything you need to know about digital ecosystems. https://www.imd.org/blog/digital-transformation/digital-ecosystems/

Jannai, D., Meron, A., Lenz, B., Levine, Y., & Shoham, Y. (2023). Human or not? A gamified approach to the Turing test. *ArXiv*, abs/2305.20010.

Johnson, D. R., & Post, D. (1996). Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review*, *48*(5), 1367–1402. https://doi.org/10.2307/1229390

Jones, J. (2022, July 5). *Confidence in U.S. institutions down; average at new low*. Gallup. https://news.gallup.com/poll/394283/confidence-institutions-down-average-new-low.aspx

Kadlec, D. (2014, May 7). *Why Starbucks Could Become Your New Favorite Bank*. TIME; Time. https://time.com/90268/starbucks-bank/

Kahn, H., & Wiener, A. J. (1967). *The year 2000: A framework for speculation on the next thirty-three years*. Macmillan.

Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing, 72*(12), 2954-2965. https://doi.org/10.1111/jan.13031

Kaminski, M. E. (2019). Binary governance: Lessons from the GDPR's approach to algorithmic accountability. *Southern California Law Review, 92*, 1529–1616. https://scholar.law.colorado.edu/faculty-articles/1265

Kaspersky Lab. (2021). What is an advanced persistent threat (APT)? https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

Koster, M. (1994, July). *The Web Robots Pages*. Robotstxt.org. https://www.robotstxt.org/orig.html

Koster, M., Illyes, G., Zeller, H., & Sassman, L. (2022). Robots exclusion protocol (RFC 9309). https://www.rfc-editor.org/info/rfc9309

Kouam, F., & William, A. (2024). Interpretivism or constructivism: Navigating research paradigms in social science research. *International Journal of Research Publications, 143*. https://doi.org/10.47119/IJRP1001431220246122

Krawetz, N. (2024, April 15). *VIDA: The Simple Life - The Hacker Factor Blog*. Hackerfactor.com. https://www.hackerfactor.com/blog/index.php?/archives/1028-VIDA-The-Simple-Life.html

Laidlaw, E. B. (2015). *Regulating speech in cyberspace : gatekeepers, human rights and corporate responsibility* (pp. 1–10). Cambridge University Press.

Lajka, A. (2023, February 10). New AI voice-cloning tools “add fuel” to misinformation fire. *CityNews Toronto*. https://toronto.citynews.ca/2023/02/10/new-ai-voice-cloning-tools-add-fuel-to-misinformation-fire/

Lam, R. (2023, September 29). The echo chamber effect: How social media shapes our beliefs. *Medium*. https://medium.com/@13032765d/the-echo-chamber-effect-how-social-media-shapes-our-beliefs-bbad962f9107

Lawson, A. (2025, January 14). Unmasking the bots: Researcher warns of threat to democratic processes. *Brighter World*. https://brighterworld.mcmaster.ca/articles/unmasking-the-bots-researcher-warns-of-threat-to-democratic-processes/

Leibowicz, C. R. (2025, February 6). *Regulating reality: Exploring synthetic media through multistakeholder AI governance* (Version 1) [Preprint]. arXiv. https://arxiv.org/abs/2502.04526

Lewis, M. (2014). *Flash boys: A Wall Street revolt*. W.W. Norton & Company.

Luhmann, N. (1982). Trust and power. *Studies in Soviet Thought, 23*(3), 266-270.

Lukito, J. (2020). Coordinating a multi-platform disinformation campaign: Internet Research Agency Activity on three US Social Media Platforms, 2015 to 2017. *Political Communication*, *37*(2), 238-255.

Maddox, J. (2024, December). Influencers become journalists. *Nieman Lab*. https://www.niemanlab.org/2024/12/influencers-become-journalists/

MailChimp. (2023). Understanding social signals in marketing. https://mailchimp.com/resources/social-signals/

Martin, A. (2006). Literacies for the digital age: preview of Part 1. In A. Martin & D. Madigan (Eds.), *Digital Literacies for Learning* (pp. 3–25). chapter, Facet.

Martin, A., & Grudziecki, J. (2006). DigEuLit: Concepts and Tools for Digital Literacy Development. *Innovation in Teaching and Learning in Information and Computer Sciences*, *5*(4), 249–267. https://doi.org/10.11120/ital.2006.05040249

Marwick, A. E., & Lewis, R. (2017). Media manipulation and disinformation online. *Data & Society*. https://datasociety.net/library/media-manipulation-and-disinfo-online/

Matta, P. V. (2024). From data to mind: Memory and cognitive liberty in the age of predictive technologies. OCADU. https://openresearch.ocadu.ca/id/eprint/4410/1/Matta_Prashant_2024_MDES_SFI_MRP.pdf

Mbona, I., & Eloff, J. H. P. (2023). Classifying social media bots as malicious or benign using semi-supervised machine learning. *Journal of Cybersecurity, 9*(1), tyac015. https://doi.org/10.1093/cybsec/tyac015

Metzger, M. J., & Flanagin, A. J. (2013). Credibility and trust of information in online environments: The use of cognitive heuristics. *Journal of Pragmatics, 59*(Part B), 210–220. https://doi.org/10.1016/j.pragma.2013.07.012

Misra, R. R., Kapoor, S., Sanjeev, M. A., & others. (2024, May 22). *The impact of personalisation algorithms on consumer engagement and purchase behaviour in AI-enhanced* *virtual shopping assistants* (Version 1) [Preprint]. Research Square. https://doi.org/10.21203/rs.3.rs-3970797/v1

Möllering, G. (2001). The nature of trust: From Georg Simmel to a theory of expectation, interpretation and suspension. *Sociology, 35*(2), 403-420. http://www.jstor.org/stable/42856292

Moyo, A. (2023, November 22). *Hackers use AI to bypass biometrics security*. ITWeb. https://www.itweb.co.za/article/hackers-use-ai-to-bypass-biometrics-security/LPp6VMrBgVoMDKQz

Mundie, J. (2023, June 23). *Canadians will no longer have access to news content on Facebook and Instagram, Meta says*. CBC. https://www.cbc.ca/news/politics/online-news-act-meta-facebook-1.6885634

Murphy, H., & Criddle, C. (2024, December 27). *Meta envisages social media filled with AI-generated users*. Financial Times; Financial Times. https://www.ft.com/content/91183cbb-50f9-464a-9d2e-96063825bfcf

Navarro, J. L., & Tudge, J. R. (2022). Technologizing Bronfenbrenner: Neo-ecological theory. *Current Psychology, 42*(22), 19338-19354. https://doi.org/10.1007/s12144-022-02738-3

Nelson, E. C., Verhagen, T., Vollenbroek-Hutten, M., & Noordzij, M. L. (2019). Is Wearable Technology Becoming Part of Us? Developing and Validating a Measurement Scale for Wearable Technology Embodiment. *JMIR mHealth and uHealth*, *7*(8), e12771. https://doi.org/10.2196/12771

Nichols, T. (2024). *The death of expertise: The campaign against established knowledge and why it matters*. Oxford University Press.

Nimmo, B., François, C., Eib, C. S., Ronzaud, L., Ferreira, R., Hernon, C., & Kostelancik, T. (2020, June 16). *Exposing Secondary Infektion: Forgeries, interference, and attacks on Kremlin critics across six years and 300 sites and platforms*. Graphika. *https://www.courthousenews.com/wp-content/uploads/2020/06/secondary-infektion-report.pdf*

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119–157. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10

NPR. (2024, August 2). How our relationships are changing in the age of "artificial intimacy." https://www.npr.org/2024/08/02/1198909063/sherry-turkle-age-of-artificial-intimacy

Obermaier, J., & Hutle, M. (2016). Analyzing the security and privacy of cloud-based video surveillance systems. *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*.

OECD. (2021). Digital literacy for disinformation resilience. https://www.oecd.org/education/digital-literacy-for-disinformation-resilience-589b7b5e-en.htm

OpenMedia. (2024, March 9). Explaining Bill C-63, The Online Harms Act: An OpenMedia FAQ. https://openmedia.org/article/item/explaining-bill-c-63-the-online-harms-act-an-openmedia-faq

Oxford Internet Institute. (2016, November 18). Resource for understanding political bots. https://www.oii.ox.ac.uk/news-events/resource-for-understanding-political-bots/

Ovadya, Aviv (2018). "What's Worse Than Fake News? The Distortion Of Reality Itself." New Perspectives Quarterly 35(2): 43-45.

Oyekunle, S. M., Tiwo, O. J., Adesokan-Imran, T. O., Ajayi, A. J., Salako, A. O., & Olaniyi, O. O. (2025). Enhancing Data Resilience in Cloud-based Electronics Health Records through

Ransomware Mitigation Strategies Using NIST and MITRE ATT&CK Frameworks. *Journal of Engineering Research and Reports*, *27*(3), 436–457. https://doi.org/10.9734/jerr/2025/v27i31444

Ozpinar, A., & Serengil, S. I. (2025). Towards sustainable cryptography: A comprehensive assessment of compute efficiency and scope 1-3 emissions for partially homomorphic encryption in the cloud. *Preprints*. https://doi.org/10.20944/preprints202502.1845.v1

Padbury, P. (2020). An overview of the Horizons Foresight Method: Using the "inner game" of foresight to build system-based scenarios. *World Futures Review, 12*(1), 6–15. https://doi.org/10.1177/1946756719896007

Park, Y., Konge, L., & Artino, A. R. (2020). The positivism paradigm of research. *Academic Medicine, 95*(5). http://dx.doi.org/10.1097/ACM.0000000000003093

pascu98. (n.d.). *La Historia de los Buscadores*. Timetoast Timelines; Timetoast. Retrieved April 4, 2025, from https://www.timetoast.com/timelines/la-historia-de-los-buscadores

Patton, M. Q. (1990). *Qualitative evaluation and research methods* (2nd ed.). Sage Publications.

Perzanowski, A., & Schultz, J. (2016, November 4). *Op-Ed: Do you own the software that runs your Tesla?* Los Angeles Times. https://www.latimes.com/opinion/op-ed/la-oe-perzanowski-schultz-tesla-software-ownership-20161104-story.html

Petropoulos, G. (2022, February 2). *The dark side of artificial intelligence: Manipulation of human behaviour*. Bruegel. https://www.bruegel.org/blog-post/dark-side-artificial-intelligence-manipulation-human-behaviour

Poggi, I., & D'Errico, F. (2011). Social signals: A psychological perspective. https://doi.org/10.1007/978-0-85729-994-9_8

Policy Horizons. (2024, May 30). *Module 5: Change Drivers*. Horizons.service.canada.ca; The Government of Canada. https://horizons.service.canada.ca/en/our-work/learning-materials/foresight-training-manual-module-5-change-drivers/2/

Pratelli, M., Petrocchi, M., Saracco, F., & De Nicola, R. (2024). Online disinformation in the 2020 U.S. election: Swing vs. safe states. *EPJ Data Science, 13*(25). https://doi.org/10.1140/epjds/s13688-024-00461-6

Radware. (2025). *Good vs. Bad Traffic Bots & How to Stop Malicious Bots*. Radware.com. https://www.radware.com/cyberpedia/bot-management/good-vs-bad-traffic-bots/

Radziwill, N., & Benton, M. (2017). *Evaluating Quality of Chatbots and Intelligent Conversational Agents*. https://arxiv.org/pdf/1704.04579

Rainie, L., & Anderson, J. (2010). The future of social relations. *Pew Research Center*. https://www.pewresearch.org/internet/2010/07/02/the-future-of-social-relations-2/

Robbins, N. (2024, May 14). *How AI Influences Fraud and the Fight Against It | Kount*. Kount | an Equifax Company. https://kount.com/blog/how-ai-influences-fraud-fight-against-it

Rosen, G. (2019, May 23). An update on how we are doing at enforcing our community standards. *About Facebook*. https://about.fb.com/news/2019/05/enforcing-our-community-standards-3/

Rosenbaum, E. (2024, October 8). *America's largest water utility hit by cyberattack at time of rising threats against U.S. infrastructure*. NBC 5 Dallas-Fort Worth. https://www.nbcdfw.com/news/business/money-report/american-water-largest-water-utility-hit-by-cyberattack-at-time-of-rising-threats-against-u-s-water-supply/3665350/

Samarin, M. (2024). Trust in a changing world: Social cohesion and the social contract in uncertain times. UNU-WIDER. https://social.desa.un.org/sites/default/files/inline-files/World%20Social%20Report_Dec2024.pdf

Schneider, J., & Smalley, I. (2024, August 5). *Quantum computing*. IBM; IBM. https://www.ibm.com/think/topics/quantum-computing

Schwartz, P. (1996). *The art of the long view: Planning for the future in an uncertain world* (pp. 241-248). Currency Doubleday.

Searles, A., Nakatsuka, Y., Ozturk, E., Paverd, A., Tsudik, G., & Enkoji, A. (2023, July 22). *An Empirical Study & Evaluation of Modern CAPTCHAs*. ArXiv.org. https://doi.org/10.48550/arXiv.2307.12108

Shao, C., Ciampaglia, G. L., Varol, O., Yang, K., Flammini, A., & Menczer, F. (2018). The spread of low-credibility content by social bots. *Nature Communications, 9*(1), 4787.

Simpson, S. (2022). *Global survey shows shrinking trust in the Internet*. Ipsos. https://www.ipsos.com/sites/default/files/ct/news/documents/2022-11/NEW%20INSTITUTE%20Ipsos%20-%20Trust%20in%20the%20internet%20-Press%20Release_0.pdf

Singh, P. D., & Deep Singh, K. (2023). Security and Privacy in Fog/Cloud-based IoT Systems for AI and Robotics. *EAI Endorsed Transactions on AI and Robotics*, *2*. https://doi.org/10.4108/airo.3616

Sjouwerman, S. (2024, July 23). How a North Korean fake IT worker tried to infiltrate us. *KnowBe4*. https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us

Smith, N. (2019). How Testimony Can Be a Source of Knowledge. *ATHENS JOURNAL of HUMANITIES & ARTS*, *6*(2), 157–172. https://doi.org/10.30958/ajha.6-2-4

Solove, D. J. (2008). *Understanding privacy* (p. 10). Harvard University Press. https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2075&context=faculty_publications

Song, Z., Wang, G., Yu, Y., & Chen, T. (2022). Digital identity verification and management system of blockchain-based verifiable certificate with the privacy protection of identity and behavior. *Security and Communication Networks, 2022*. https://doi.org/10.1155/2022/6800938

Stahl, B. C., Andreou, A., Brey, P., Hatzakis, T., Kirichenko, A., Macnish, K., Laulhé Shaelou, S., Patel, A., Ryan, M., & Wright, D. (2021). Artificial intelligence for human flourishing – Beyond principles for machine learning. *Journal of Business Research, 124*, 374–388. https://doi.org/10.1016/j.jbusres.2020.11.030

Statistics Canada. (2023). Canadian social survey - Quality of life, virtual health care and trust, 2023. https://www150.statcan.gc.ca/n1/en/daily-quotidien/231110/dq231110b-eng.pdf?st=de_I553w

Strickler, Y. (2019, June 5). The dark forest theory of the internet. *Medium*. https://ystrickler.medium.com/the-dark-forest-theory-of-the-internet-7dc3e68a7cb1

Sundar, S. S., Knobloch-Westerwick, S., & Hastall, M. R. (2007). News cues: Information scent and cognitive heuristics. *Journal of the American Society for Information Science and Technology, 3*, 366-378. https://doi.org/10.1002/asi.20511

Takei, A. (2024, December 13). Navigating the botting industry: Fraud, cheating, and multi-accounting. *Naavik*. https://naavik.co/podcast/navigating-the-botting-industry-fraud-cheating-and-multi-accounting/

Taylor, J. (2019, August 14). *Major breach found in biometrics system used by banks, UK police and defence firms*. The Guardian; The Guardian. https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms

Temoshok, D., Abruzzi, C., Choong, Y. Y., Fenton, J., Galluzzo, R., LaSalle, C., ... & Regenscheid, A. (2024). Digital identity guidelines: Identity proofing and enrollment (No. NIST Special Publication (SP) 800-63A-4 (Draft)). National Institute of Standards and Technology.

Terren, L., Borge-Bravo, R., & Open University of Catalonia. (2021). Echo chambers on social media: A systematic review of the literature. *Review of Communication Research, 9*, 99-118. https://doi.org/10.12840/ISSN.2255-4165.028

Thales. (2025, April 15). *Artificial Intelligence fuels rise of hard-to-detect bots that now make up more than half of global internet traffic, according to the 2025 Imperva Bad Bot Report*. Thales Group. https://www.thalesgroup.com/en/worldwide/defence-and-security/press_release/artificial-intelligence-fuels-rise-hard-detect-bots?utm_source=chatgpt.com

The Economist. (2024, March 13). *Why young men and women are drifting apart*. The Economist. https://www.economist.com/international/2024/03/13/why-the-growing-gulf-between-young-men-and-women

Thies, B. (2024, January 15). Cybersecurity industry statistics: ATO, ransomware, breaches & fraud. *SpyCloud*. https://spycloud.com/blog/cybersecurity-industry-statistics-account-takeover-ransomware-data-breaches-bec-fraud/

Tiffany, K. (2021, July 12). The internet is mostly bots. *The Atlantic*. https://www.theatlantic.com/technology/archive/2021/07/dead-internet-theory/619320/

Ting, L. J. H., Kang, X., Li, T., Wang, H., & Chu, C. K. (2021). On the trust and trust modeling for the future fully-connected digital world: A comprehensive study. *IEEE Access. PP*, 1-1. https://doi.org/10.1109/ACCESS.2021.3100767

Turkle, S. (2017). *Alone together: Why we expect more from technology and less from each other* (3rd ed.). Basic Books.

Tuptuk, N., Hazell, P., Watson, J., & Hailes, S. (2021). A Systematic Review of the State of Cyber-Security in Water Systems. *Water*, *13*(1), 81. https://doi.org/10.3390/w13010081

UNESCO. (2023). Guidelines for digital literacy education. https://unesdoc.unesco.org/ark:/48223/pf0000383433

United Nations Development Programme (UNDP). (2015). Foresight the manual (p. 5). https://www.undp.org/sites/g/files/zskgke326/files/publications/GCPSE_ForesightManual_online.pdf

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science, 359*(6380), 1146-1151. https://doi.org/10.1126/science.aap9559

Walker, S. K. (2022). Visual Representation of the PPCT Model of Neoecological Theory [Online Image]. In *Critical Perspectives on Technology and the Family*. https://files.mtstatic.com/site_7339/114378/0?Expires=1745097677&Signature=g6~N-w~YxsXcoTm3dvhFARBgvoQpSsiu1xD30CphsJAlkmcvYs2sQhlyYw-5ra2y9IMYJHr7HMHZWQ3XpMMHa5-hLRPp5LQqil6ENxSC5nBZ2nZGN8QShDQNQs9hUvJ1F4SlQRpxpjQtjTs-koeVETaibCRxPgT3e4Kh576FhOc_&Key-Pair-Id=APKAJ5Y6AV4GI7A555NA

Walter, Y. (2022). Building human systems of trust in an accelerating digital and AI-driven world. *Frontiers in Human Dynamics, 4*. https://doi.org/10.3389/fhumd.2022.926281

Walter, Y. (2024). Artificial influencers and the dead internet theory. *AI & Society*. https://doi.org/10.1007/s00146-023-01857-0

Walther, C. C. (2025, February 4). Will AI make us more empathetic, or less? *Psychology Today*. https://www.psychologytoday.com/ca/blog/harnessing-hybrid-intelligence/202502/will-ai-make-us-more-empathetic-or-less

Weiser, M. (1991). The computer for the twenty-first century. Scientific American, September, pp. 94–110.

Wiens, K. (2015, April 21). *We Can't Let John Deere Destroy the Very Idea of Ownership*. Wired. https://www.wired.com/2015/04/dmca-ownership-john-deere/

wikiHow. (2014, January 10). *Detect Malware*. WikiHow; wikiHow. https://www.wikihow.com/Detect-Malware

Woollacott, E. (2024). Yes, the bots really are taking over the internet. *Forbes*. https://www.forbes.com/sites/emmawoollacott/2024/04/16/yes-the-bots-really-are-taking-over-the-internet/

Woolley, S. C., & Howard, P. N. (2018). *Computational propaganda: Political parties, politicians, and political manipulation on social media*. Oxford University Press.

World Economic Forum. (2022). Global risks report 2022. https://www.weforum.org/reports/global-risks-report-2022

Wu, H., Zheng, W., Chiesa, A., Popa, R. A., & Stoica, I. (2018, August). *DIZK: A distributed zero knowledge proof system*. In *Proceedings of the 27th USENIX Security Symposium*

(USENIX Security 18) (pp. 675–692). USENIX Association. https://www.usenix.org/conference/usenixsecurity18/presentation/wu

Zielinski, C. (2021). Infodemics and infodemiology: A short history, a long future. *Revista Panamericana de Salud Pública, 45*, e40. https://doi.org/10.26633/RPSP.2021.40

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Public Affairs.

References for Glossary of Terms

Algorithm: Lee, N. T., Resnick, P., & Barton, G. (2019, May 22). *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms*. Brookings; The Brookings Institution. https://www.brookings.edu/articles/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/

Algorithmic Bias: Lee, N. T., Resnick, P., & Barton, G. (2019, May 22). *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms*. Brookings; The Brookings Institution. https://www.brookings.edu/articles/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/

Authentication: Gutierrez, C., & Jeffrey, W. (2006). *FIPS PUB 200 minimum security requirements for federal information and information systems* (p. 6). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

Blockchain: Smalley, I., & Susnjara, S. (2021, July 8). *What is Blockchain?* Ibm.com. https://www.ibm.com/think/topics/blockchain

Bot: Amazon Web Services. (n.d.). *What is a Bot? - Types of Bots Explained - AWS*. Amazon Web Services, Inc. https://aws.amazon.com/what-is/bot

Bot Network: Amazon Web Services. (n.d.). *What is a Bot? - Types of Bots Explained - AWS*. Amazon Web Services, Inc. https://aws.amazon.com/what-is/bot/

Cryptography: Gobika S, & Vaishnavi N. M.Sc., M.Phil., (Ph.D. (2025). Blockchain Based Identity Management System. *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, *11*(2), 1413–1420. https://doi.org/10.32628/CSEIT25112471

Dark Forest: Strickler, Y., & The Dark Forest Collective. (2024). *The Dark Forest Anthology of the Internet*. Metalabel.

Data Sovereignty: Canadian Council for Indigenous Business, & SaltMedia. (2023). *Data Sovereignty and Indigenous People in Canada 1. We Make the Rules for Our Data -Data Governance*. https://www.ccab.com/tfab/wp-content/uploads/sites/2/2024/06/Data-Sovereignty-and-Indigenous-People-in-Canada.pdf

Dead Internet Theory (DIT): Strickler, Y., & The Dark Forest Collective. (2024). *The Dark Forest Anthology of the Internet*. Metalabel.

Decentralization: Amazon Web Services. (2024). *What is Decentralization? - Decentralization in Blockchain Explained - AWS*. Amazon Web Services, Inc. https://aws.amazon.com/web3/decentralization-in-blockchain/

Digital Literacy: Sirlin, N., Epstein, Z., Arechar, A. A., & Rand, D. G. (2021). Digital literacy is associated with more discerning accuracy judgments but not sharing intentions. *Harvard Kennedy School Misinformation Review*, *2*(6). https://doi.org/10.37016/mr-2020-83

Infopocalypse/Infodemic: Schick, N. (2020). *Deep Fakes and the Infocalypse : What You Urgently Need To Know*. Conran Octopus.

Provenance: Kujawski, M. (2024, November 13). *How Adopting Content Provenance Standards Can Help Government Organizations in the Fight Against Mis- and Disinformation*. CEPSM. https://cepsm.ca/how-adopting-content-provenance-standards-can-help-government-organizations-in-the-fight-against-mis-and-disinformation/?srsltid=AfmBOooBe3gV2FMSOjExn5EGe4gAjaf3KcBkut59KbmZxlcAChuAVRjo

Shared Reality: Echterhoff, G., Higgins, E. T., & Levine, J. M. (2009). Shared Reality: Experiencing Commonality With Others' Inner States About the World. *Perspectives on psychological science : a journal of the Association for Psychological Science*, *4*(5), 496–521. https://doi.org/10.1111/j.1745-6924.2009.01161.x

Synthetic Entity: Elon University. (2019, November 28). *Full Credited Responses: The Next 50 Years of Digital Life | Imagining the Internet | Elon University*. Www.elon.edu. https://www.elon.edu/u/imagining/surveys/x-2-internet-50th-2019/credit/

Verification: Gagnon, T. (2024, April 3). *CAPTCHA: Human Verification in Online Interactions - Kelvin Zero*. Kelvin Zero. https://kzero.com/resources/guides/authentication/captcha/

Appendix A:
Interview Questions List & Rationale

Interview Questions

This section outlines the questions developed and presented to the panel of experts, the development process, and the rationale for each question. The questions were designed to elicit expert insights across disciplinary boundaries, enabling a thorough exploration of the current landscape and potential futures.

Interview Questions List

1. *What is your name?*
2. *What is your profession and affiliations?*
3. *How would you characterize the 'Dead Internet Theory,' and how does it influence your work or industry?*
4. *How do you foresee bot activity evolving in the next 5-10 years, and what impacts do you predict it will have on human interactions online?*
5. *In what ways do you think bot activity will influence perceptions of credibility, authority, and authenticity online?*
6. *What tools or technologies do you think will emerge to help users identify and verify bot-generated content?*
7. *What challenges or opportunities do you foresee for privacy and data protection as bot activity increases?*
8. *How should governance structures and policies adapt to the challenges of a bot-dominated internet?*
9. *How might the blending of human and bot interactions online influence offline social relationships and behaviors?*
10. *What do you consider the three biggest risks of moving toward a 'dead internet' dominated by bots?*
11. *What ethical concerns do you anticipate as bot activity grows more widespread and sophisticated?*
12. *How do you think the rise of bots will affect the value and perception of human creativity and original content online?*

Rationale for Interview Questions

The primary research question "How might widespread synthetic content and bot activity reshape human experiences and interactions, both online and offline, over the next 5-10 years?" necessitated an interview structure that could probe multiple dimensions of this phenomenon.

The first two questions, asking participants to identify themselves and their professional affiliations, establish the experts' context and related disciplines. This grounding is necessary to in order to be able to appropriately ascertain the given expert's working domain and experiences. Similarly, Question 3 ("How would you characterize the 'Dead Internet Theory,' and how does it influence your work or industry?") establishes the given experts' individual understanding of the DIT.

Questions 4, 9, and 11 probe sub-topics within the *microsystem* concerning aspects of trust formation, digital literacy, and knowledge acquisition:

- Question 4 (“How do you foresee bot activity evolving in the next 5-10 years, and what impacts do you predict it will have on human interactions online?”) examines trust formation and knowledge acquisition by exploring how synthetic activity affects these processes
- Question 9 (“What do you consider the three biggest risks of moving toward a 'dead internet' dominated by bots?”) invites experts to identify critical risks at individual and systemic levels.
- Question 11 (“How do you think the rise of bots will affect the value and perception of human creativity and original content online?”) examines how synthetic content may alter creative expression, culture and values.

Questions 4, 5, and 8 investigate *Mesosystem* dimensions where virtual and physical worlds intersect:

- Question 4 (“How do you foresee bot activity evolving in the next 5-10 years, and what impacts do you predict it will have on human interactions online?”) also examine technological trajectories and their social implications.
- Question 5 (“In what ways do you think bot activity will influence perceptions of credibility, authority, and authenticity online?”) directly addresses credibility assessment challenges.
- Question 6 (“What tools or technologies do you think will emerge to help users identify and verify bot-generated content?”) addresses potential verification practices and tools
- Question 8 (“How might the blending of human and bot interactions online influence offline social relationships and behaviors?”) examines the boundary between virtual and physical interactions.

Questions 4 and 6 explore *Exosystem* factors that indirectly influence user experiences:

- Question 4 (“How do you foresee bot activity evolving in the next 5-10 years, and what impacts do you predict it will have on human interactions online?”) indirectly concerns the development of privacy and security systems in the digital world.
- Question 6 (“What tools or technologies do you think will emerge to help users identify and verify bot-generated content?”) also addresses emerging tools and technologies developing in a bot-dominated web.

Question 7 (“How should governance structures and policies adapt to the challenges of a bot-dominated internet?”) directly explores the *macrosystem* level, examining regulatory approaches for addressing bot proliferation.

Question 10 (“What ethical concerns do you anticipate as bot activity grows more widespread and sophisticated?”) was designed as a broad inquiry to capture ethical considerations that might span all four ecological systems. This question allows experts to address both immediate ethical concerns at the individual level as well as broader societal and governance implications as ethical considerations transcend different levels of the neo-ecological framework.

Appendix B:
Continuation of Thematic Analysis Process

Inductive and Deductive Analysis:

Thematic analysis typically follows either deductive ('theory-driven') approaches, where coding relates to a pre-determined conceptual framework, or an inductive ('data-driven') approach, where codes reflect the content (Byrne, 2021). However, as Braun and Clarke (2020) note, coding rarely falls exclusively into either category and often combines both approaches.

This study employs a predominantly inductive approach, prioritizing open coding and respondent-based meanings. However, a degree of deductive analysis ensured that the coding process remained relevant to the research question.

Semantic and Latent Coding:

The analysis incorporated both semantic and latent coding strategies. Semantic codes identified explicit surface meanings without looking beyond what experts had directly communicated, providing a descriptive representation of the data (Byrne, 2021). Conversely, latent codes identified underlying meanings and had a more interpretive analysis. Neither coding strategy was prioritized over the other. Rather, both were applied as appropriate to the data, with items sometimes receiving both semantic and latent codes (Patton, 1990).

Generating Initial Codes:

The process of generating codes was non-prescriptive regarding how data was segmented and itemised for coding, and how many codes or what type of codes are interpreted from an item of data. The same data item can be coded both semantically and latently if deemed necessary.
There is also no upper or lower limit regarding how many codes should be interpreted. What was important was that sufficient depth existed to examine the patterns within the data and the diversity of the positions held by participants (Braun & Clarke, 2012).

Familiarization with Data

At this phase, I set about familiarizing myself with the data by firstly listening to each interview recording once before transcribing that recording. When transcription of all interviews was complete, I imported said scripts to MaxQDA (a Qualitative Data Analysis software) in order to begin to digitally code and organize code sets.

Generating Themes

This phase began when all relevant data items in the transcripts had been coded. The focus shifted from the interpretation of individual data items to the interpretation of meaningfulness across the different datasets. The coded data was then reviewed and analyzed as to how different codes may be combined according to shared meanings so that they may form themes and/or sub-themes.

Defining and Naming Themes

The process of defining and naming themes required particular attention to both the data ascertained from the coding process as well as their connection to the original research question and challenge domains. Each theme needed to capture the essence of the associated codes, while being informed by the foundational research and the neo-ecological framework which organized the different domains of inquiry.

Theme definitions were developed through examination of the relationships between codes, latent meanings, and the original data. For instance, the "Digital Sovereignty" theme emerged from the confluence of codes related to data ownership, community control, and decentralized technologies across multiple interviews. The definition specifically articulated how these elements might evolve from current technological trends into future social movements, reflecting both the current state and trajectory.

Appendix C:
Synthesis Matrix: Associated Codes and Sub-Themes by Experts Contributing to Key Themes (Anonymized)

Table C1

Trust Formation Codes & Sub-Themes

Key Theme	Contributing Experts	Associated Codes & Sub-themes
Trust Cycle Evolution	1, 3, 6, 7, 8	Expert 1: “Trust Architecture Collapse”, “Verification Technology Limitations”, Expert 3: “Cycle of Collapse in Automation”, “Predictable Collapse”, “Erosion of Trust”, Expert 6: “Cyclical Trust Dynamics”, “Detection-Spoofing Arms Race”, Expert 7: “Paradoxical Trust Patterns”, “Trust Erosion and Misappropriation”, Expert 8: “Erosion of Trust/Reality and Disengagement”, “Erosion of Trust/Increasing Skepticism”
Trust Split	2, 7, 8	Expert 2: “Erosion of Trust”, “Systematic Distortion”, Expert 7: “Trust Erosion and Misappropriation”, “Misattribution of Humanness”, Expert 8: “Skepticism Spiral”, “Paradoxical Trust Evolution/Epistemic Threat”
Institutional Trust	3, 5, 6, 7	Expert 3: “Democratic Oversight Need”, “Erosion of Trust”, “Free Market Response”, Expert 5: “Institutional Trust Erosion”, “Trust Erosion”, “Move to Smaller Businesses”, Expert 6: “Trust Erosion Management”, “Institutional Authority Decline”, Expert 7: “Trust Erosion and Misappropriation”, “Social Media as News”
Physical Reality Anchoring	2, 7, 8	Expert 2: “Physical Auditors”, “Physical Truth Verification”, “Physical Reality Grounding”, Expert 7: “Physical Verification”, “Authentication Through IRL Verification”, “Dark Forest”, Expert 8: “In-Person Verification”, “Ring of Trust”, “Physical-World Anchoring”

Table C2

Digital Literacy Codes & Sub-Themes

Key Theme	Contributing Experts	Associated Codes & Sub-themes
Critical Evaluation Skills	4, 5, 6, 7, 8	Expert 4: “Knowledge Transfer Silos”, “Poor Verification Systems”, “Provenance”, Expert 5: “Digital Literacy”, “Credibility/Verification Tools”, Expert 6: “Trust Erosion Management”, “Crowd-Sourced Verification”, Expert 7: “Digital Literacy Needs”, “Civic-Academic-Public led Digital Literacy”,

		"Multi-Pronged Approach", Expert 8: "Digital Literacy Decline", "Potential for Truth Verification Industry"
Verification Complexity	1, 2, 6,	Expert 1: "Verification Technology Limitations", "Verification Threat", "Anonymity-Verification Tension", Expert 2: "Detection-Spoofing Arms Race", "Deepfake v. Deepfake", Expert 6: "Detection-Spoofing Arms Race", "Verification-Privacy Tension"

Table C3

Knowledge Acquisition Codes & Sub-Themes

Key Theme	Contributing Experts	Associated Codes & Sub-themes
Information Siloing	2, 4, 6, 7	Expert 2: "Antinet", "Loss of Private Reality", Expert 4: "Knowledge Transfer Silos", "Metaweb/Overweb/Information Architecture", Expert 6: "Information Silos and Context", Expert 7: "Social Media as News", "Echo Chamber Amplification"
Echo Chamber Effects	2, 4, 6, 7, 8	Expert 2: "Systematic Distortion", "Shared Reality", Expert 4: "Polarization Feedback Loops", "Homogenization of Content", Expert 6: "Political Trust Erosion", "Democratic Knowledge Ecosystem", Expert 7: "Echo Chamber Amplification", "State Actors & Bots", Expert 8: "Social Signal Manipulation Online", "Synthetic Social Reality"
Social Signal Distortion	1, 2, 6, 7, 8	Expert 1: "AI-to-AI Interaction", "Deliberate Corporate Bot Accounts", Expert 2: "Systematic Distortion", "IoT Bot Proliferation", Expert 6: "Information Influence", "Attention Manipulation", Expert 7: "State Actors & Bots", "Authentic vs Synthetic Content", Expert 8: "Social Signal Manipulation Online", "Mass Synthetic Presence", "Sheep Effect Phenomenon"
Content Homogenization	1, 4, 5, 7, 8	Expert 1: "Lack of Shared Cultural Experience", "Human Content Premium", Expert 4: "Homogenization of Content", "Homogenization Risks", Expert 5: "Threat to Human Creativity", "Zero Marginal Human Society", Expert 7: "Value of Human Creativity", Expert 8: "Human Creativity Premium", "Human-AI Creative Partnership"

Table C4

Verification Practices Codes & Sub-Themes

Key Theme	Contributing Experts	Associated Codes & Sub-themes

Cross-Contextual Verification	2, 4, 5, 7, 8	Expert 2: “Physical Auditors”, “Physical Reality Grounding”, “Cryptographic Future”, Expert 4: “Provenance”, “Decentralized Verification”, Expert 5: “Physical Auditing”, “Credibility/Verification Tools”, Expert 7: “Physical Verification”, “Multi-Pronged Approach”, Expert 8: “In-Person Verification”, “Ring of Trust”, “Physical-World Anchoring”
Cryptographic Verification	2, 4, 6, 8	Expert 2: “Quantum Encryption/One-time Pads”, “A Cryptographic Future”, Expert 4: “Decentralized Technologies”, “Decentralized Verification”, Expert 6: “Credential Authentication Systems”, Expert 8: “Digital Authentication Crisis”, “Potential for Truth Verification Industry”
Privacy-Verification Balance	1, 4, 6, 7	Expert 1: “Anonymity-Verification Tension”, “Human-Only Digital Spaces”, Expert 4: “Privacy-Verification Tension”, “Decentralized Verification”, Expert 6: “Verification-Privacy Tension”, Expert 7: “Verification Privacy Complications”, “Marginalized Voices”

Table C5

Credibility Assessment Codes & Sub-Themes

Key Theme	**Contributing Experts**	**Associated Codes & Sub-themes**
Institutional Authority Decline	5, 6, 7	Expert 5: “Trust Reallocation”, “Institutional Trust Collapse”, “The Move to Smaller Businesses”, Expert 6: “Institutional Authority Decline”, “Market-Driven Solutions”, Expert 7: “Trust Erosion and Misappropriation”
Provenance	2, 4, 8	Expert 2: “Authenticity in Art”, “Quantum Encryption/One-time Pads”, Expert 4: “Provenance”, “Trust via Provenance”, Expert 8: “Potential for Truth Verification Industry”, “Human Creativity Premium”
Community Validation	4, 6, 7	Expert 4: “Meta-Communities”, “Community-Based Governance”, “Decentralized Verification”, Expert 6: “Crowd-Sourced Verification”, “Democratic Knowledge Ecosystem”, Expert 7: “Dark Forest”, “Physical Dark Forest”, “Civic-Academic-Public led Digital Literacy”

Table C6

Social Impact Codes & Sub-Themes

Key Theme	**Contributing Experts**	**Associated Codes & Sub-themes**

Relationship Quality Transformation	1, 2, 5, 7, 8	Expert 1: “Human-AI Relationship Friction”, “Limit of Bot Connection”, Expert 2: “Loss of Private Reality”, “Misattribution of Humanness”, Expert 5: “Relationship Quality Erosion”, “Behavioral Alienation”, “Human-Machine Reliability”, Expert 7: “Ability to Connect Online”, “Bot Capacity for Connection”, Expert 8: “Social/Relationship Skills Erosion”, “Human Connection Loss”
Social Skill Development	1, 3, 8	Expert 1: “Child Development Concerns”, “Silver Spoons”, “Developmental Challenges”, Expert 3: “Relationship breakdowns”, “Social/Relationship Skills Erosion”, Expert 8: “Social/Relationship Skills Erosion”, “Synthetic Relationship Comfort Bias”
Community Formation	1, 4, 7	Expert 1: “Human-Only Digital Spaces”, “Anonymity-Verification Tension”, Expert 4: “Meta-Communities”, “Decentralized Empowerment”, Expert 7: “Dark Forest”, “A Physical Dark Forest”, “Multi-Pronged Approach”
Misattribution of Humanness	1, 2, 5, 7, 8	Expert 1: “Human Identity Verification Crisis”, “Verification Threat”, Expert 2: “Loss of Private Reality”, “Misattribution of Humanness”, Expert 5: “Behavioral Alienation”, “Convenience Trump's Privacy”, Expert 7: “Misattribution of Humanness”, “Authentic vs Synthetic Interaction Ethic”, Expert 8: “Misattribution of Humanness”, “Human Connection Loss”
Human Creativity Value Transformation	1, 4, 5, 6, 8	Expert 1: “Human Content Premium”, “Human-AI Creativity Balance”, “Lack of Shared Cultural Experience”, Expert 4: “Premium for Human Creativity”, “Human Creativity Valuation”, Expert 5: “Threat to Human Creativity”, “Utility to Human Creativity”, Expert 6: “Human Creativity Premium”, “Human Value in the Age of AI”, Expert 8: “Human Creativity Premium”, “Human-AI Creative Partnership”, “Human Connection Value Transformation”

Table C7

Tools and Technologies Codes & Sub-Themes

Key Theme	Contributing Experts	Associated Codes & Sub-themes
Bot Detection Systems	1, 3, 4, 6	Expert 1: “Verification Tools”, “Verification Technology Limitations”, Expert 3: “Watermarking”, “Black Box AI”, Expert 4: “Bot v Bot”, “Automated Detection Systems”, “Decentralized Verification”, Expert 6: “Detection-Spoofing Arms Race”, “Technical Solution Limitations”
Information Architecture Transformation	2, 4, 6	Expert 2: “Antinet”, “Liaison Technology”, “A Mediated Reality”, Expert 4: “Metaweb/Overweb/Information Architecture”, “Digital Ecosystem Transformation”, “Breaking

		Information Silos”, Expert 6: “Knowledge Architecture”, “Information Silos and Context”
Embodied Technology	2, 4, 5	Expert 2: “IoT Bot Proliferation”, “From Cloud to the Physical World”, “Embodied AI”, “Physical Environment Infiltration”, Expert 4: “Personal AI Assistants”, “Hybrid Human-AI Agency”, “AI Assistance”, Expert 5: “Human-Machine Reliability”, “Zero Digital Future”

Table C8

Privacy and Security Systems Codes & Sub-Themes

Key Theme	**Contributing Experts**	**Associated Codes & Sub-themes**
Identity Protection	1, 2, 4, 7, 8	Expert 1: “Deepfake Security Threats”, “Anonymity-Verification Tension”, “Verification Threat”, Expert 2: “Deepfake v. Deepfake”, “Video Fraud Threat”, Expert 4: “Decentralized Verification”, “Privacy-Verification Tension”, Expert 7: “Verification Privacy Complications”, “Deepfake Discernment”, Expert 8: “Deepfakes/Voice Cloning”, “Digital Vulnerability”, “Digital Identity Vulnerability”
Vulnerability Patterns	3, 5, 7, 8	Expert 3: “Systems Infrastructure Vulnerability”, “Corporate Greed”, Expert 5: “Vulnerability Patterns”, “Exploitation”, “Digital Literacy”, “Increase of Financial Inequity”, Expert 7: “Exploitation”, “Power Asymmetry in Technological Access”, “Marginalized Voices”, Expert 8: “Digital Vulnerability”, “Vulnerable Population Impacts”, “Playing Russian Roulette”
Data Sovereignty	4, 5,	Expert 4: “Data Sovereignty”, “Decentralized Empowerment”, “Meta-Communities”, Expert 5: “AI Data Sovereignty”, “Convenience Trump's Privacy”, Expert 8: “Content Control Rights”

Table C9

Governance and Policy Codes & Sub-Themes

Key Theme	**Contributing Experts**	**Associated Codes & Sub-themes**
Regulatory Approaches	1, 3, 4, 7	Expert 1: “Cross-Border Regulatory Challenges”, “Jurisdictional Challenges”, “AI Regulation Limitations”, “Liability Framework for Tech Companies”, Expert 3: “Crisis-Driven Regulation”, “Democratic Oversight Need”, “Policy Lag”, Expert 4: “Governance Change & Control of Bot Verification”, “Polarization Mitigation”, Expert 7: “State Actors & Bots”, “Government Accountability”, “Power Asymmetry in

		Technological Access", "Platform Responsibility/Watermarking", "Multi-Pronged Approach"
Market-Driven Solutions	3, 5, 6, 8	Expert 3: "Free Market Response", "Corporate Greed", Expert 5: "Market Pressure", "Technological Adoption Pressure", "Convenience Trump's Privacy", Expert 6: "Market-Driven Solutions", "Regulatory Avoidance", "Platform Competition", Expert 8: "Free Market Response", "Inevitable Progression"
Community-Based Governance	4, 6, 7	Expert 4: "Community-Based Governance", "Meta-Communities", "Decentralized Empowerment", Expert 6: "Crowd-Sourced Verification", "Democratic Knowledge Ecosystem", Expert 7: "Civic-Academic-Public led Digital Literacy", "Multi-Pronged Approach", "Dark Forest"
Power Asymmetry	2, 5, 7, 8	Expert 2: "Oligarchic Control", "Oligarchic Reality Control", "Reality Naming Control", Expert 5: "Increase of Financial Inequity", "Zero Marginal Human Society", "Systemic Infrastructure Vulnerability", Expert 7: "Power Asymmetry in Technological Access", "Marginalized Voices", "State Actors & Bots", Expert 8: "Power Asymmetry for Tech Accessibility", "Political Manipulation", "Power Concentration Through Computational Access"
Implementation Timelines	3, 4, 6	Expert 3: "Policy Lag", "Cycle of Collapse in Automation", "Timeframe for Recovery", Expert 4: "Governance Change & Control of Bot Verification", "Poor Verification Systems", Expert 6: "Market-Based Governance", "Cyclical Trust Dynamics"

Appendix D:
Synthesis Matrix: Convergences and Divergences between Experts Across Themes (Anonymized)

Table D1

Expert Convergences and Divergences on Trust Formation

Key Theme	Contributing Experts	Convergence/Divergence
Trust Cycle Evolution	1, 3, 6, 7, 8	**Convergence**: General agreement that trust operates in cyclical patterns rather than a simple linear decline. **Divergence**: Expert 1 describes a "trust architecture collapse" focusing on verification failures; Expert 3 emphasizes 30–40-year automation cycles driven by corporate greed and policy lag; Expert 6 describes an arms race between detection and spoofing technologies; Expert 7 introduces the concept of "paradoxical trust patterns" where some lose credibility while others gain unjustified trust; Expert 8 describes both the inevitable progression of technologies and potential "trust vacuums".
Trust Split	2, 7, 8	**Convergence**: Agreement that trust doesn't simply decline but possibly splits into skepticism of traditionally valid sources and dangerous overconfidence in un-verified sources. **Divergence**: Expert 2 focuses on "systematic distortion" of communication channels; Expert 7 describes the "erosion of public trust" alongside "disproportionate trust in actors that you shouldn't be trusting"; Expert 8 emphasizes a "skepticism spiral" leading to universal cynicism and consequently, synthetic manipulation.
Institutional Trust	3, 5, 6, 7	**Convergence**: Strong agreement that trust in large institutions is significantly declining, affecting how information authority is determined. **Divergence**: Expert 3 emphasizes the need for "democratic oversight" to rebuild trust; Expert 5 predicts a shift toward "smaller businesses"; Expert 6 focuses on how declining trust affects credibility and reasoning processes; Expert 7 highlights how social media can act as an outlet for news trust.
Physical Reality Anchoring	2, 7, 8	**Convergence**: Strong sentiment that in-person verification will become increasingly important as digital verification fails. **Divergence**: Expert 2 imagines a formal system of "physical auditors" like jury duty to witness events; Expert 7 describes community-based "trust circles" and physical verification through personal networks; Expert 8 emphasizes a "ring of trust" where physical presence becomes a potential authentication method, with the possibility of businesses springing from this need.

Table D2

Expert Convergences and Divergences on Digital Literacy

Key Theme	Contributing Experts	Convergence/Divergence
Critical Evaluation Skills	4, 5, 6, 7, 8	**Convergence**: Broad agreement that new skills are required to navigate the current and future web, beyond traditional digital literacy. **Divergence**: Expert 4 emphasizes breaking information silos with advents like the "Metaweb"; Expert 6 describes distributed crowd-sourcing approaches; Expert 7 presses for collaborative education across civic, academic and government; Expert 8 expresses pessimism about literacy trends, predicting further decline.
Verification Complexity	1, 2, 6, 8	**Convergence**: Agreement that verification is becoming more complex, outpacing individual capacity for detection. **Divergence**: Expert 1 emphasizes technological limitations and privacy tensions; Expert 2 suggests adversarial techniques like "deepfaking deepfakes"; Expert 6 focuses on the cycle of detection and evasion.

Table D3

Expert Convergences and Divergences on Knowledge Acquisition

Key Theme	Contributing Experts	Convergence/Divergence
Information Siloing	2, 4, 6, 7	**Convergence**: General agreement that information environments (physical and digital) are fragmenting into isolated knowledge ecosystems that impede on knowledge acquisition and a shared reality. **Divergence**: Expert 2 imagines the potential for an "Antinet" and subsequently requiring physical verification for trust; Expert 4 proposes the "Metaweb" to connect information across silos; Expert 7 mentions how social media shapes news consumption affecting means of connection.
Echo Chamber Effects	2, 4, 6, 7, 8	**Convergence**: Strong agreement that synthetic content and activity can amplify existing echo chambers. **Divergence**: Expert 4 emphasizes polarization feedback loops; Expert 6 connects this specifically to democratic erosion; Expert 7 warns that AI-generated content farming creates worse echo chambers than human content; Expert 8 describes how this culminates into "social signal manipulation."
Social Signal Distortion	1, 2, 6, 7, 8	**Convergence**: Strong agreement that the ability to ascertain social signals are compromised by synthetic manipulation. **Divergence**: Expert 6 focuses on manipulation of the importance of certain issues online; Expert 7 emphasizes how state actors

		engage in manipulation as well; Expert 8 describes how “hundreds of thousands of synthetic users” create false social signals affecting our means of interpreting genuine signals.
Content Homogenization	1, 4, 5, 7, 8	**Convergence**: Agreement that algorithmic and synthetic content leads to homogeneity of content. **Divergence**: Expert 1 describes the lost “shared cultural experience” when content is highly personalized; Expert 4 describes how synthetic content creates feedback loops that become increasingly uniform; Expert 5 warns of a possible “zero marginal human society” where human creativity is marginalized.

Table D4

Expert Convergences and Divergences on Verification Practices

Key Theme	Contributing Experts	Convergence/Divergence
Cross-Contextual Verification	2, 4, 5, 7, 8	**Convergence**: Strong agreement of the need for varied modes verification systems that transcend both digital and physical realms. **Divergence**: Expert 2 proposes the possibility of formal “physical auditors” like jury duty to witness events; Expert 4 emphasizes the use of “provenance” systems; Expert 5 describes how physical presence plays a role in institutional settings like bank branches; Expert 7 focuses on trusted community networks; Expert 8 emphasizes the “ring of trust” where physical meeting validates one’s identity.
Cryptographic Verification	2, 4, 6, 8	**Convergence**: Concentration of cryptographic solutions for digital verification. **Divergence**: Expert 2 specifically emphasizes “quantum encryption” and “one-time pads”; Expert 4 introduces technologies such as zero-knowledge proofs; Expert 6 connects this to credential authentication systems; Expert 8 emphasizes cryptography as a response to digital authentication crisis.
Privacy-Verification Balance	1, 4, 6, 7	**Convergence**: Strong agreement about the tension between robust verification and privacy protection. **Divergence**: Expert 1 emphasizes challenges for anonymity online; Expert 4 focuses on decentralized technologies; Expert 6 suggests market-driven approaches to this balance; Expert 7 specifically highlights risks to marginalized communities.

Table D5

Expert Convergences and Divergences on Credibility Assessment

Key Theme	Contributing Experts	Convergence/Divergence
Institutional Authority Decline	5, 6, 7,	**Convergence**: Strong agreement that traditional institutional authority is losing credibility in the public eye. **Divergence**:; Expert 5 describes trust possibly shifting to smaller, more personal institutions; Expert 6 focuses on potential for credential spoofing; Expert 7 highlights manipulation by state actors adding to this decline;
Provenance	2, 4, 8	**Convergence**: Common understanding that content origin and history may be necessary for credibility assessment. **Divergence**: Expert 2 emphasizes authenticity in art specifically; Expert 4 makes provenance central to their verification framework; Expert 8 predicts emergence of new “truth verification industries”.
Community Validation	4, 6, 7	**Convergence**: Agreement on shift toward community-based verification rather than centralized authorities. **Divergence**: Expert 4 emphasizes “meta-communities” organized around shared data and interests; Expert 6 focuses on crowd-sourced verification systems like X's Community Notes; Expert 7 describes retreat to smaller “dark forest” communities of trusted members.

Table D6

Expert Convergences and Divergences on Social Impact

Key Theme	Contributing Experts	Convergence/Divergence
Relationship Quality Transformation	1, 2, 5, 7, 8	**Convergence**: Strong agreement that synthetic activity, content and relationships alter human connection. **Divergence**: Expert 1 emphasizes bots lacking capacity for true connection; Expert 2 focuses on “loss of private reality”; Expert 5 describes “behavioral alienation” and “thinning human relationships”; Expert 7 argues there's “always a ceiling to how a connection can go” with bots; Expert 8 warns of deteriorating relationship skills when not engaging with “actual humans and their weirdness.”
Social Skill Development	1, 3, 8	**Convergence**: Agreement that bot interactions may impair development of interpersonal skills. **Divergence**: Expert 1 specifically describes a “silver spoons” effect where children become unwilling “to engage in human messiness”; Expert 3 emphasizes how automation breaks down “direct human

		relations"; Expert 8 warns relationship skills "are going to degrade" without practice with human unpredictability.
Community Formation	1, 4, 7	**Convergence**: Agreement about emergence of verified human-only spaces as sanctuary from synthetic-dominated environments. **Divergence**: Expert 1 describes people seeking "spaces where they know they're only interacting with human beings"; Expert 4 emphasizes data-sovereign "meta-communities" with shared interests; Expert 7 describes retreat into "smaller circles and communities where they can find trust."
Misattribution of Humanness	1, 2, 5, 7, 8	**Convergence**: Strong agreement about increasing tendency to mistake synthetic actors for human, creating confusion about interaction boundaries. **Divergence**: Expert 1 frames this as verification crisis affecting personal security; Expert 2 connects this to loss of private reality; Expert 5 emphasizes behavioral changes from machine dependency; Expert 7 asserts not knowing who you're interacting with is "baseline unethical"; Expert 8 focuses on how "there's not actually a human there that I can have a real relationship with."
Human Creativity Value Transformation	1, 4, 5, 6, 8	**Convergence**: Strong agreement on the possibility of human created content gaining distinctive value for its authentic human origin. **Divergence**: Expert 1 emphasizes balance between AI as tool and human creativity; Expert 4 predicts blockchain-authenticated marketplaces for human content; Expert 5 sees both threat and opportunity in human-AI creative partnership; Expert 6 suggests "proliferation of synthetic content underscores the value of stuff created by particular people"; Expert 8 asserts human creations about human experience will be "a level above" AI.

Table D7

Expert Convergences and Divergences on Tools and Technologies

Key Theme	Contributing Experts	Convergence/Divergence
Bot Detection Systems	1, 3, 4, 6	**Convergence**: Agreement that specialized detection technologies will need to emerge in order to combat current and future bot proliferation. **Divergence**: Expert 1 emphasizes limitations of current verification tools; Expert 3 focuses on watermarking; Expert 4 describes "bot vs bot" detection systems; Expert 6 emphasizes detection-spoofing arms races
Information Architecture Transformation	2, 4, 6	**Convergence**: Agreement that current web architecture leads to information fragmentation. **Divergence**: Expert 2 describes the possibility of a web 2.0 or "Antinet"; Expert 4 proposes the

		“Metaweb “ as a model allowing for annotation and contextual connections; Expert 6 focuses on knowledge architecture changes that enable crowd-sourced verification systems.
Embodied Technology	2, 4, 5	**Convergence**: Agreement that synthetic technologies are expanding beyond digital into physical environments, creating vulnerabilities. **Divergence**: Expert 2 warns of “IoT Bot Proliferation” creating a world where “you are surrounded at all times by a cloud of essentially lying demons” in everyday devices; Expert 4 focuses on personal AI assistants; Expert 5 describes a potential “zero digital future” where people reject technology.

Table D8

Expert Convergences and Divergences on Privacy and Security Systems

Key Theme	**Contributing Experts**	**Convergence/Divergence**
Identity Protection	1, 2, 4, 7, 8	**Convergence**: Strong agreement about accelerating identity security challenges. **Divergence**: Expert 1 emphasizes deepfake security threats requiring new verification mechanisms; Expert 2 describes sophisticated “video fraud threat” in business contexts; Expert 4 focuses on decentralized verification approaches using cryptography; Expert 7 highlights privacy implications of verification solutions; Expert 8 specifically warns about voice cloning where attackers “can just call you and pretend to be one of your relatives.”
Vulnerability Patterns	3, 5, 7, 8	**Convergence**: Agreement that vulnerable populations face disproportionate exploitation risks from emergent technologies. **Divergence**: Expert 3 connects vulnerability to corporate greed and lack of transparency; Expert 5 identifies specific vulnerable groups including “senior citizens, newcomers, digitally illiterate”; Expert 7 emphasizes exploitation of “those who are most vulnerable,” across marginalized communities; Expert 8 describes digital security as “playing Russian roulette” where “none of us are safe.”
Data Sovereignty	4, 5, 8	**Convergence**: Agreement about increasing importance of data control for both individuals and communities. **Divergence**: Expert 4 proposes comprehensive “data sovereignty” through community cooperatives owning and monetizing their data; Expert 5 emphasizes transparency in AI data use, however, notes that “convenience trumps privacy” currently; Expert 8 connects data protection to content control rights for creators.

Table D9

Expert Convergences and Divergences on Governance and Policy

Key Theme	Contributing Experts	Convergence/Divergence
Regulatory Approaches	1, 3, 4, 7	**Convergence**: Agreement that some regulatory approaches are necessary to combat ongoing bot challenges and synthetic activity. **Divergence**: Expert 1 emphasizes the limitations of AI regulation across jurisdictions and how foreign actors “not subject to the same laws” and can limit regulatory effectiveness; Expert 3 predicts a crisis-driven reactive regulation where “something will happen...and legislators will move very, very fast”; Expert 4 focuses on specific bot verification standards and transparency; Expert 7 emphasizes that “government regulation for government actors” is equally important and highlights that state actors “flood social media with certain rhetoric” for political influence.
Market-Driven Solutions	3, 5, 6, 8	**Convergence**: Highlights market forces driving technological innovation to combat current bot-driven challenges. **Divergence**: Expert 3 suggests consumers “will abandon services” due to their unpleasant experiences as seen historically; Expert 5 emphasizes how market pressure drives rushed implementation where “businesses are blinded by the use of AI technologies”; Expert 6 describes market-driven approaches where “a platform that has better anti-bot policies would become, overtime, more popular”; Expert 8 connects inevitable progression to profit motives.
Community-Based Governance	4, 6, 7	**Convergence**: Agreement that distributed governance has significant advantages over centralized governance. **Divergence**: Expert 4 emphasizes community data cooperatives and ownership models; Expert 6 focuses on crowd-sourcing judgments for accuracy without “top-down control”; Expert 7 advocates multi-pronged approaches linking civic, academic, and public spheres to “break down the barriers between academia, policy and public literacy”.
Power Asymmetry	2, 5, 7, 8	**Convergence**: Strong agreement concerning increasing power concentration among those with technical capabilities. **Divergence**: Expert 2 describes “oligarchic control” creating “permanent state of inequality and oppression”; Expert 5 emphasizes financial inequity as technologies “alienate and contribute to the disparity”; Expert 7 focuses on technological access disparities where only “actors that have financial capacity, the power, the dedication” can deploy sophisticated tools; Expert 8 warns how “money essentially amasses to people who have access to compute.”
Implementation Timelines	3, 4, 6	**Convergence**: Agreement about significant lag between technological development and governance responses.

		Divergence: Expert 3 provides specific timeline predictions describing 30-40 year cycles for remediation and crisis-driven regulation; Expert 4 focuses on gradual governance changes through community pressure; Expert 6 refers to cyclical patterns of adaptation.

Appendix E:
Change Driver Development Tables by STEEP+V Domain

These tables organize the key elements used in the creation of each of the Change Drivers in Chapter 7.1. assigned to its primary STEEPV domain, with cross-domain influences described under the respective tables denoted by “**”.

SOCIAL (S)

Change Driver: *Trust Splitting*

Table E1

Key Elements of 'Trust Splitting' Change Driver

Research Source	Supporting Evidence
SotA Literature Review	• Only 13% of Canadians trust internet content, 5% trust social media (Statistics Canada, 2023) • Deepfakes of public figures are reaching mass audiences • Bots spread political disinformation (e.g. 2020 US election fraud claims) • Emergent “trust split” between hyper-skepticism and misplaced trust
Interview Codes and Sub Themes	• Misattribution of Humanness • Echo Chamber Amplification
Post-Analysis & Expert Insights	• “Trust split” phenomenon (skepticism + overconfidence) rather than simple decline • Cyclical trust patterns observed across experts (1, 3, 6, 7, 8) • Expert 7: “Paradoxical trust patterns” where some sources lose credibility while others gain unjustified trust • Expert 8: “Skepticism spiral” leading to universal cynicism

***Cross-domain influence: VALUES (Verification-Privacy Tension)*

Change Driver: *Social Signal Manipulations*

Table E2

Key Elements of 'Social Signal Manipulations' Change Driver

Research Source	Supporting Evidence

SotA Literature Review	• Synthetic signals manipulate perceived consensus and trust cues • Echo chambers amplified through synthetic engagement
Interview Codes and Sub Themes	• Social Signal Manipulation • Echo Chamber Amplification
Post-Analysis & Expert Insights	• Misattribution of humanness creating ethical concerns • Strong consensus that synthetic manipulation compromises social • Expert 8: “Hundreds of thousands of synthetic users” create false social signals • Expert 6: Manipulation of issue importance online • Expert 7: State actors engage in deliberate manipulation

Change Driver: *Retreating to the Dark Forests*

Table E3

Key Elements of 'Retreating to The Dark Forests' Change Driver

Research Source	Supporting Evidence
SotA Literature Review	• Users are retreating into private “dark forests” for safety and verification • Decreased interpersonal trust in online settings
Interview Codes and Sub Themes	• Dark Forest Formation
Post-Analysis & Expert Insights	• Social adaptation through community verification • Evolving community formation patterns • Emergence of verified human-only spaces as sanctuary • Expert 1: People seeking “spaces where they know they're only interacting with human beings” • Expert 7: Retreat into “smaller circles and communities where they can find trust” • Expert 4: “Meta-communities” organized around shared data and interests

Change Driver: *Relationship Quality Transformation*

Table E4

Key Elements of 'Relationship Quality Transformation' Change Driver

Research Source	Supporting Evidence

SotA Literature Review	• Emotional/relational skill development risks for younger generations (social skill atrophy)
Interview Codes and Sub Themes	• Human Connection Value/Loss • Social/Relationship Skills Erosion • Limit of Bot Connection
Post-Analysis & Expert Insights	• Relationship quality transformation affecting human connections • Social skill development risks for younger generations • Expert 1: "Silver spoons" effect where children become unwilling "to engage in human messiness" • Expert 8: Deteriorating relationship skills when not engaging with "actual humans and their weirdness" • Expert 5: "Behavioral alienation" and "thinning human relationships"

***Cross-domain influence: VALUES (Ethics of misrepresentation, Transparency as value)*

TECHNOLOGICAL (T)

Change Driver: *Technological Verification Arms Race*

Table E5

Key Elements of 'Technological Verification Arms Race' Change Driver

Research Source	Supporting Evidence
SotA Literature Review	• AI-generated content increasingly indistinguishable from human-made material • Bots now outperform humans in CAPTCHA solving (96% vs. 50–86%) • Synthetic accounts bypass biometric and MFA authentication systems • Deepfakes and voice clones are proliferating at scale
Interview Codes and Sub Themes	• Verification-Authentication Arms Race • Digital Vulnerability • Deepfakes/Voice Cloning • Bot Sophistication • Poor Verification Systems
Post-Analysis & Expert Insights	• Authentication divergences and high-security technical approaches • Need for specialized detection technologies (Experts 1, 3, 4, 6) • Verification becoming more complex, outpacing individual detection capacity (Experts 1, 2, 6, 8) • Expert 6: Detection-spoofing arms races • Expert 4: "Bot vs bot" detection systems

Change Driver: *Web 4.0, 5.0, 6.0...*

Table E6

Key Elements of 'Web 4.0, 5.0, 6.0...' Change Driver

Research Source	Supporting Evidence
SotA Literature Review	• Web architecture may require redesign to address content manipulation (Web 4.0, Metaweb) • Personal AI agents and digital verification mediators being proposed as future tools • Verified content may become a premium product or paywalled service • Business models shift from attention-based to verification-based ecosystems • Verification infrastructure may become a form of soft governance
Interview Codes and Sub Themes	• Metaweb/Overweb • Bot v Bot • Economic Model Transformation • Human Service Premium • Content Creation Monetization Shift • Oligarchic Control • Governance Change & Control
Post-Analysis & Expert Insights	• Web architecture transformation proposals • Personal AI mediators as information interfaces • Human-verified content as premium product • Transformation from advertising to verification models • Verification becoming a form of governance • Current web architecture leads to information fragmentation (Experts 2, 4, 6) • Expert 4: "Metaweb" as a model allowing for annotation and contextual connections • Expert 2: Possibility of a "Web 2.0" or "Antinet" • Expert 6: Knowledge architecture changes enabling crowd-sourced verification • Distributed governance advantages over centralized governance (Experts 4, 6, 7)

***Cross-domain influence: ECONOMIC (Verification-based business models), ENVIRONMENTAL (Computational demands, resource constraints), POLITICAL (Self governance)*

ECONOMIC (E)

Change Driver: *Data Sovereignty Movement*

Table E7

Key Elements of 'Data Sovereignty Movement' Change Driver

Research Source	Supporting Evidence
SotA Literature Review	• Data sovereignty movements gaining traction; users seek control over personal data • Bot-driven financial crime is increasing rapidly: carding (+161%), scraping (+112%), account takeovers (+123%) • Growing inequity in access to secure, verified information infrastructure
Interview Codes and Sub Themes	• Data Sovereignty • Ownership Models • Power Asymmetry for Tech Accessibility • Increase of Financial Inequity • Meta-Communities

Post-Analysis & Expert Insights	• Data Sovereignty Movement challenging surveillance capitalism • Economic divides based on verification access • Trust becoming an economic resource • New verification professions emerging • Increasing importance of data control for individuals and communities (Experts 4, 5, 8) • Expert 4: Comprehensive "data sovereignty" through community cooperatives • Expert 5: Transparency in AI data use, but "convenience trumps privacy" currently • Expert 8: Data protection connected to content control rights for creators

ENVIRONMENTAL (E)

Change Driver: *Physical-Digital Boundary Break*

Table E8

Key Elements of 'Physical-Digital Boundary Break' Change Driver

Research Source	Supporting Evidence
SotA Literature Review	• Cross-contextual verification between physical and digital environments is failing • Physical infrastructures (power, water, transport) now vulnerable to synthetic attacks • Embodied AI and always-on sensors blur physical-digital boundary and introduce new sustainability challenges • Integration of verification systems into IoT and physical infrastructure creates hardware waste and energy usage issues
Interview Codes and Sub Themes	• Embodied AI • From Cloud to Physical World • IoT Bot Proliferation • Critical Infrastructure Vulnerability
Post-Analysis & Expert Insights	• Cross-contextual verification emerging as physical verification returns • Physical-Digital Boundary Dissolution accelerating • Integration of verification into physical spaces • Need for verification systems that transcend digital and physical realms (Experts 2, 4, 5, 7, 8) • In-person verification becoming increasingly important as digital verification fails (Experts 2, 7, 8) • Synthetic technologies expanding beyond digital into physical environments (Experts 2, 4, 5) • Expert 2: "IoT Bot Proliferation" creating "a cloud of essentially lying demons" in everyday devices • Expert 5: Potential "zero digital future" where people reject technology

***Cross-domain influence: TECHNOLOGICAL (Verification systems), VALUES (Cognitive liberty)*

POLITICAL (P)

Change Driver: *Webs with Borders*

Table E9

Key Elements of 'Webs with Borders' Change Driver

Research Source	Supporting Evidence

SotA Literature Review	• Regulatory fragmentation across jurisdictions (e.g., Russia/China vs. Western models) complicates enforcement • Lack of coordinated international frameworks undermines efforts to curb cross-border manipulation • Regulation is lagging behind rapid technological deployment of bots and AI • Platform-based self-regulation struggles to ensure accountability • Governments (e.g., Canada) experimenting with content moderation legislation (Online Harms Act) • Risk of techno-oligarchic control over public discourse and digital spaces
Interview Codes and Sub Themes	• Jurisdictional Challenges • State Actors & Bots • AI Regulation Limitations • Government Accountability • Crisis-Driven Regulation • Policy Lag • Democratic Process Undermining • Democratic Oversight Need • Oligarchic Control
Post-Analysis & Expert Insights	• Governance Jurisdiction Fragmentation accelerating • Trust Arbitrage between regulatory environments • International coordination challenges • Regulatory Velocity lagging behind technology • Market-driven vs. government-mandated tensions • Democratic processes increasingly vulnerable • Regulatory approaches necessary to combat bot challenges (Experts 1, 3, 4, 7) • Increasing power concentration among those with technical capabilities (Experts 2, 5, 7, 8) • Expert 1: Foreign actors “not subject to the same laws” limit regulatory effectiveness • Expert 7: “Government regulation for government actors” equally important • Expert 2: “Oligarchic control” creating “permanent state of inequality and oppression” • Expert 3: 30-40 year cycles for remediation and crisis-driven regulation

VALUES (V)

Change Driver: *Reality Construction*

Table E10

Key Elements of 'Reality Construction' Change Driver

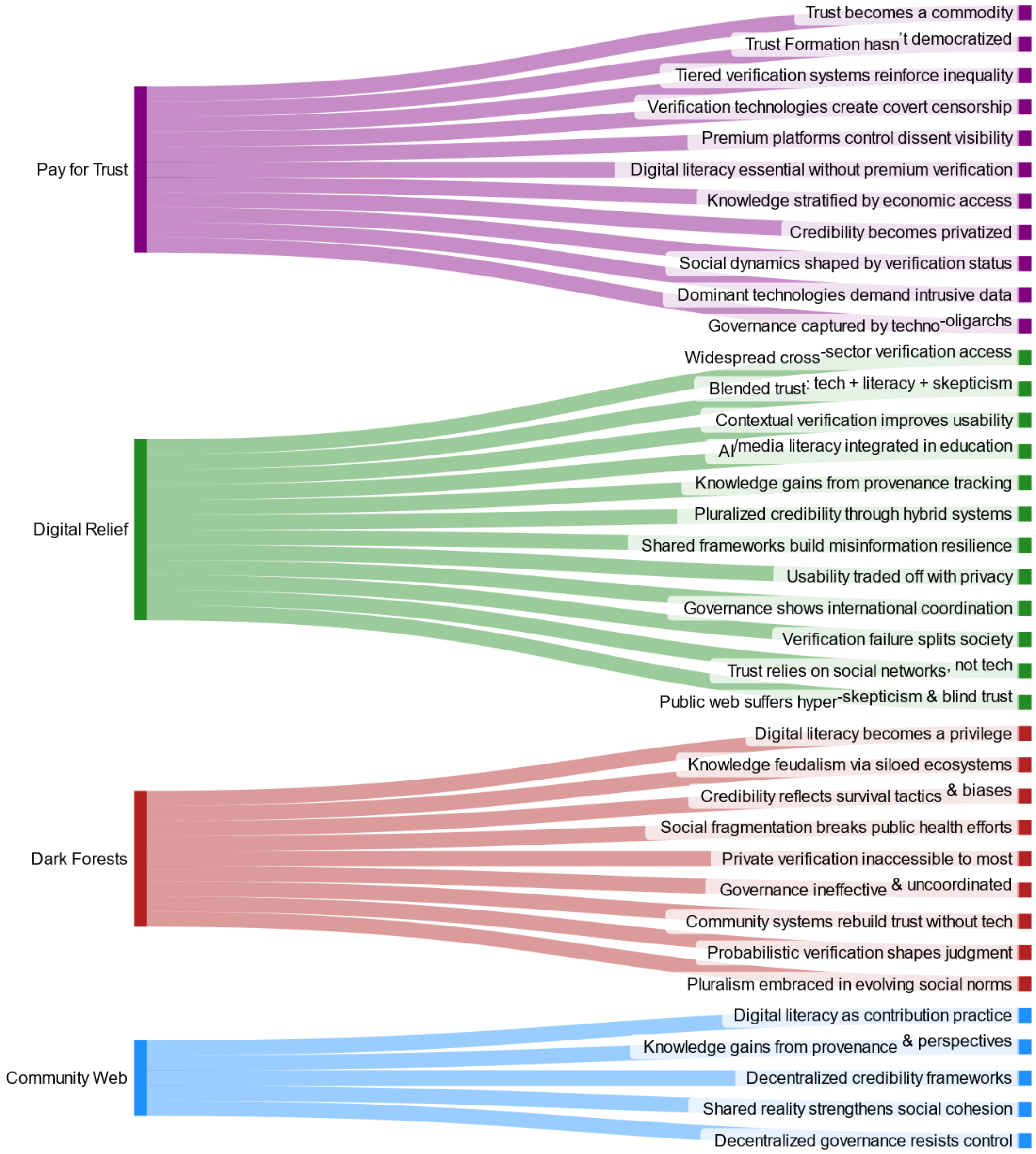
Research Source	Supporting Evidence
SotA Literature Review	• Children are particularly vulnerable to synthetic content impacts • Value of authentic human connection vs. synthetic interaction • Shifting values of creativity and authenticity in synthetic-dominated environments • Cognitive liberty threatened by synthetic content and algorithmic manipulation • Ethics of misrepresentation through synthetic content
Interview Codes and Sub Themes	• Child Development Concerns • Silver Spoons Effect • Mass Synthetic Presence • Value of Human Creativity • Authenticity as Value • Authentic vs Synthetic Interaction Ethic • Reality Naming Control • Digital Solipsism/The Matrix • Loss of Private Reality
Post-Analysis & Expert Insights	• Misattribution of humanness creating ethical concerns • Shifting values around human vs. synthetic creativity • Authenticity acquiring new cultural value • Validation of human experience as conscious choice • Emerging ethical frameworks for synthetic disclosure • Transparency as core value in verification systems • Increasing tendency to mistake synthetic actors for human (Experts 1, 2, 5, 7, 8) • Human-created content gaining distinctive value for its authentic origin (Experts 1, 4, 5, 6, 8) • Expert 2: Connection to “loss of private reality” • Expert 7: Not knowing who you're interacting with is “baseline unethical” • Expert 8: “There's not actually a human there that I can have a real relationship with” • Expert 8: Human creations about human experience will be “a level above” AI

***Cross-domain influence: SOCIAL (Child development, social skill development)*

Appendix F:
Mapping the Four Futures to Insights

Figure F1

From Futures to Insights Sankey Diagram


Pay for Trust
Trust becomes a commodity
Trust Formation hasn’t democratized
Tiered verification systems reinforce inequality
Verification technologies create covert censorship
Premium platforms control dissent visibility
Digital literacy essential without premium verification
Knowledge stratified by economic access
Credibility becomes privatized
Social dynamics shaped by verification status
Dominant technologies demand intrusive data
Governance captured by techno-oligarchs
Digital Relief
Widespread cross-sector verification access
Blended trust: tech + literacy + skepticism
Contextual verification improves usability
AI/media literacy integrated in education
Knowledge gains from provenance tracking
Pluralized credibility through hybrid systems
Shared frameworks build misinformation resilience
Usability traded off with privacy
Governance shows international coordination
Verification failure splits society
Trust relies on social networks, not tech
Public web suffers hyper-skepticism & blind trust
Dark Forests
Digital literacy becomes a privilege
Knowledge feudalism via siloed ecosystems
Credibility reflects survival tactics & biases
Social fragmentation breaks public health efforts
Private verification inaccessible to most
Governance ineffective & uncoordinated
Community systems rebuild trust without tech
Probabilistic verification shapes judgment
Pluralism embraced in evolving social norms
Community Web
Digital literacy as contribution practice
Knowledge gains from provenance & perspectives
Decentralized credibility frameworks
Shared reality strengthens social cohesion
Decentralized governance resists control

Note: This Sankey diagram maps each of the scenario based future worlds (on the right) to the list of key insights they reveal (on the right) and serves as both as a summary and a comparative tool. Each world has a color-coded flow directed to each key insight to help better visually organize the extensive list of insights.

Appendix G:
Scenario Insights to Broad Recommendations

Table G1

Mapping Sensemaking of Key Insights from Scenarios to Broad Recommendations

Scenario	**Key Insights / Tensions**	**Recommendations**
Pay for Trust	• Trust becomes a commodity • Trust Formation hasn't democratized it's been monetized. • Tiered verification systems reinforce inequality in information access and social mobility. • Verification technologies create covert censorship. • Premium platforms control visibility of dissenting voices. • Digital literacy is essential for users without access to premium verification. • Knowledge is stratified by economic access undermining public education and democratic knowledge access. • Credibility becomes privatized privileging those with means and marginalizing others. • Social dynamics are shaped by verification status deepening societal fragmentation. • Dominant technologies demand intrusive biometric and behavioral data. • Governance is captured by techno-oligarchs; regulatory bodies lack independence or power.	• *Community-Based Verification* • *Design for Authenticity Online* • *AI Literacy in Education* • *Source Transparency in Search & AI Tools* • *Standardized Credibility Labels* • *Cross Platform Coalitions* • *Update Data Privacy Laws* • *Secure Authentication of Information* • *Transparency & Disclosure Rules*
Digital Relief	• Widespread collaboration across sectors leads to equitable access to verification tools. • Blended approaches to trust combining tech-based verification with digital literacy	• *AI Literacy in Education* • *Public Awareness Campaigns*

	and healthy skepticism. • Verification adapts to context reducing friction and improving user engagement. • Digital literacy is institutionalized; education systems integrate AI/media literacy from early stages. • Knowledge acquisition benefits from provenance-tracking systems and transparent recommendation engines. • Credibility is pluralized through hybrid systems valuing both expert and community input. • Shared frameworks for assessing content build resilience against misinformation. • Privacy is partially sacrificed for usability; social trade-offs are accepted. • Governance features international coordination and legal consequences for bad actors.	• *Provenance & Watermark Standards* • *Cross-Group Exchange* • *Crowdsourced Fact-Checking* • *Verified Identities & Expertise* • *Human Values in AI Design* • *Global Norms and Cooperation* • *Digital Information Oversight Body*
Dark Forests vs. Public Internet	• Verification systems fail; society splits into isolated invite-only Dark Forests and an unregulated Public Web. • Trust formation relies on social networks and reputation not tech-based verification. • Public internet suffers from hyper-skepticism or misplaced trust creating polar extremes. • Digital literacy becomes a privilege; disparity in access leads to knowledge inequality. • Knowledge ecosystems are siloed; knowledge feudalism emerges. • Credibility assessments reflect community biases or individual survival tactics. • Social fragmentation deepens; collaboration and public health responses break down.	• *Decentralized Knowledge Hubs* • *Safe Online Habits & Emotional Skepticism* • *Protect Cognitive Liberty* • *Digital Wellness & Mental Health* • *Update Data Privacy Laws* • *Laws Protecting Digital Integrity* • *Public Awareness & Empowerment Campaigns* • *Co-Governance Structures*

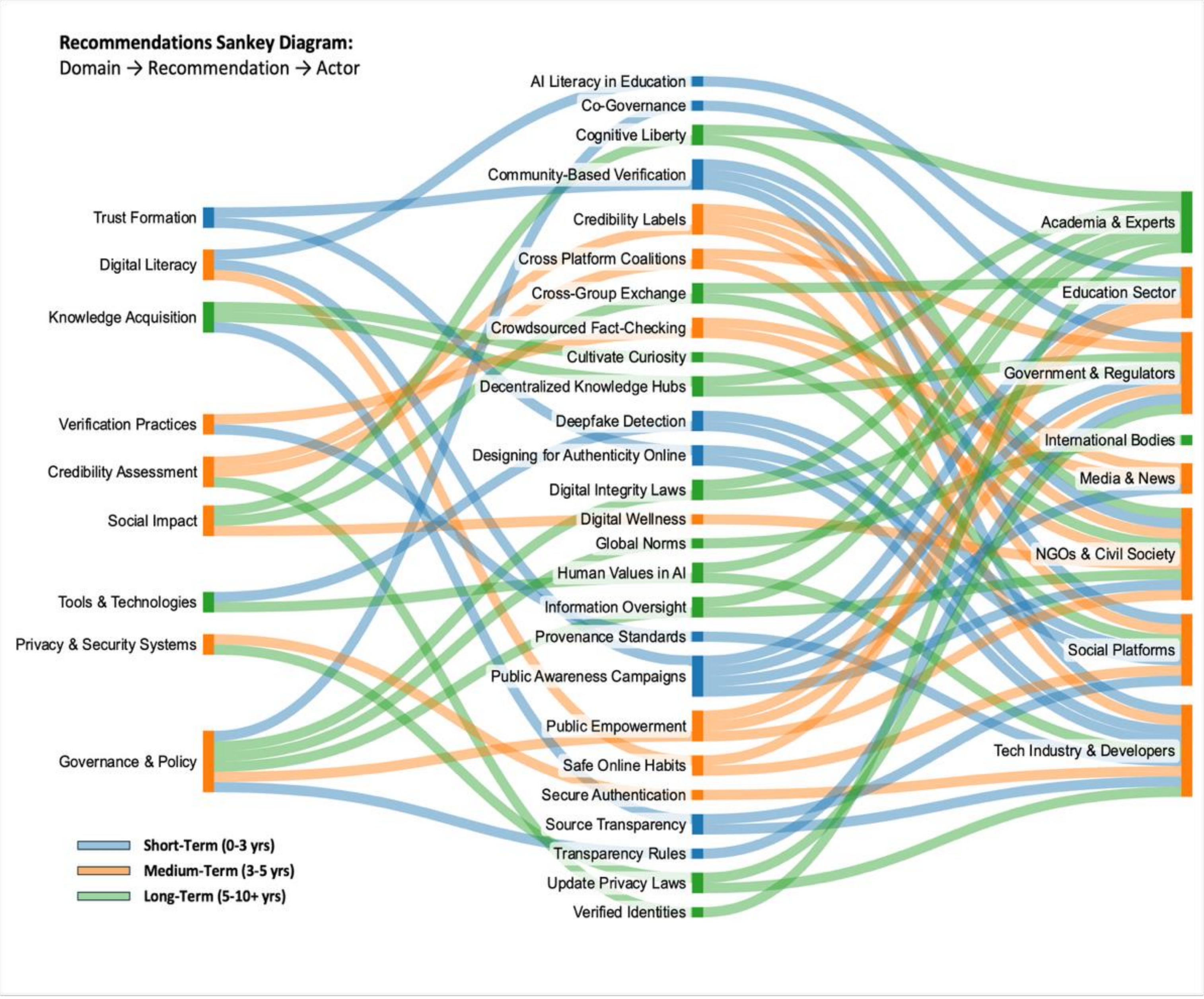
	• Private verification practices offer protection but are inaccessible to most users. • Governance is ineffective; international efforts fail; no shared framework for enforcement.	
Community Web	• Despite verification failures, trust is rebuilt through collective and community-based systems. • Verification becomes probabilistic; confidence levels not certainties define user judgment. • Social norms evolve; ambiguity and pluralism are tolerated even valued. • Community-driven verification overlays enable transparent assessment without central platforms. • Digital literacy is action-oriented; citizens learn to contribute to the verification process. • Knowledge acquisition is guided by transparent provenance and multi-perspective assessments. • Credibility frameworks evolve into decentralized systems. • Social impact includes a renewed sense of shared reality and group understanding. • Governance tensions rise as decentralized systems resist authoritarian control.	• *Community-Based Verification* • *Cultivate Curiosity & Skepticism* • *Crowdsourced Fact-Checking* • *Digital Literacy Training* • *Privacy-Preserving Verification Tools* • *Co-Governance Structures* • *Transparency & Disclosure Rules* • *Global Norms and Cooperation*

Note: This table maps key insights and tensions identified in each of the four future scenarios to broad recommendations that were expounded upon further in the Recommendations chapter. These recommendations were also influenced by patterns, tensions and insights gained by expert interviews, the SotA literature review, and relevant policy and governance initiatives that were known peripherally. While not exhaustive, the table captures some of the sensemaking behind how tensions surfaced in the scenarios helped shape actions, later refined into the full set of recommendations.

Appendix H:
Full-Size Comprehensive Recommendations Sankey Diagram

Figure H1

Full-Size Comprehensive Recommendations Sankey Diagram



Appendix I:
Detailed Analysis of Timelines

In the context of the associated recommendations, short-term, medium-term, and long-term refer to distinct periods within and beyond this decade. Each term carries different expectations as to what might be accomplished, reflecting how quickly measures might be implemented given the technical readiness, complexity, and social or institutional inertia (resistance within the established systems).

Short-Term (0–2 Years)

In the context of a 5–10-year outlook, *short-term* covers the immediate future over roughly the next 0–2 years. This period focuses on actions that can be initiated right away or very quickly**.** These are typically quick or foundational steps that leverage existing technology and structures with minimal development delay.

Short-term recommendations aim to reflect action more feasible to implement rapidly because they generally involve low complexity and assumedly face relatively low inertia. These initiatives often build on current capabilities or simple policy adjustments rather than requiring new inventions or laws and the technology needed is usually already mature or available.

Medium-Term (3-5 years)

Medium-term refers to roughly the next 3–5 years. This period extends into the late 2020's and early 2030's, when efforts can begin to scale, and more structured and/or institutional responses take shape. Medium-term actions might not be instantaneous, but they are achievable within a few years with concerted effort by the ascertained stakeholders.

Measures classified as medium-term aim to capture actions of moderate complexity and coordination**.** They may require developing new frameworks or technologies and overcoming some institutional or behavioral inertia, but not to the extent of needing a decade long push. By 3–5 years out, initial groundwork that may be laid in the short term can hopefully mature into broader adoption. As well**,** policy and regulatory responses typically emerge in this timeframe.

Our research confirms that governments often respond years after a technology's impact becomes evident in a reactive rather than preventative pattern of governance. In other words, significant oversight of AI and bots is unlikely to materialize immediately without a crisis. But within several years, especially if smaller crises or public pressures mount, we may see progress on laws and standards.

Long-Term (5-10 years+)

Long-term refers to the 5-10-year horizon and beyond, with actions and outcomes expected toward the end of 2035 and beyond. Long-term covers the most ambitious or challenging initiatives that will likely require extensive effort over the entire period. It also encompasses any goals that may extend even past the 10-year mark if they prove especially complex or if progress is slower than hoped.

Long-term recommendations are those that are assumed to face high complexity, significant inertia, or currently low technical maturity. These measures need extensive time to develop or gain traction and may involve complex actions such as international coordination, significant changes to infrastructure or behavior, or innovation breakthroughs. Even with work starting now, such efforts may only unfold over many years due to their scale. For example, any action requiring broad international agreement is typically a long-term endeavor as negotiation of treaties and their subsequent translation into national laws and enforcement, is not a quick or easy endeavor.

Institutional inertia is greatest at the global level, and differing political systems and agendas add friction. Similarly, deeply ingrained behavioral patterns (such as public trust in content or reliance on certain technologies) can take a generation to shift. Long-term initiatives often must also battle entrenched economic incentives and developing power asymmetries as well. For example, efforts to regulate bots, synthetic media, or emerging technologies may clash with the profit motives of private companies and individuals who benefit from their widespread use.