Government Information Quarterly 42 (2025) 102024

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

IT-embedded dynamic capabilities for public institutions coping with disinformation – The case of financial fake news

Oliver Rath *, Frederic Haase, Johannes Werner Melsbach, Jiarun Liu, Detlef Schoder

University of Cologne, Albertus-Magnus-Platz, Cologne 50923, Germany

ARTICLE INFO

Keywords:
Disinformation
Fake news
Taxonomy
Dynamic capabilities
Detection
Deterrence
Education

ABSTRACT

Disinformation campaigns have become a significant concern for public institutions across various domains, including politics, healthcare, and financial markets. Consequently, authorities must develop effective strategies and measures to combat such campaigns while upholding their objectives of serving the public. In financial markets, institutions aim to ensure consumer protection and market integrity, both of which are at risk due to fraudulent activities driven by financial fake news (FFN). Drawing on a sample of FFN cases and institutional communications, our study contributes to the conceptualization of FFN schemes through a taxonomy, identifies IT-embedded dynamic capabilities (DCs) and the underlying microfoundations that institutions employ to address such schemes, and discusses open challenges for institutions. Our research provides practical value for institutions, regulators, and the public by informing them about FFN schemes and offering guidance applicable to other sectors affected by disinformation, such as healthcare and politics.

1. Introduction

In recent years, several financial market (FM) institutions have issued warnings and reported on their litigation cases involving disinformation in fake news (FN). In 2022, the US Securities and Exchange Commission (SEC) suspended trading for several companies that intentionally mislead investors, e.g., regarding claims of successful deals of COVID-19 test kits, and published an alert on the wider pattern of such fake claims (U.S. Securities and Exchange Commission (SEC), 2022; U.S. Securities and Exchange Commission Investor.gov (SEC), 2022). False and misleading information has been disseminated to lure investors in the expansion of facilities and operational capabilities for cannabis production (U.S. Securities and Exchange Commission (SEC), 2023), and in 2024, scammers made use of artificial intelligence (AI) deepfakes of public figures in the UK seemingly advertising a platform for trading cryptocurrencies, reaching a broad audience in social media (Sellman, 2024). In the political domain, the European Union recently stepped up warnings about disinformation in FN ahead of major European elections and improved regulatory measures on online platform providers ordering them to help combat disinformation campaigns (Goujard, 2024). Disinformation refers to deliberately false information created and shared with the intent to mislead or manipulate people on various media channels and online platforms (Lazer et al., 2018; Nasery et al., 2023; Zhou & Zafarani, 2020). The rapid growth of digital technologies and social media platforms has facilitated the spread of disinformation amplifying its dissemination and its potential consequences (Vosoughi et al., 2018). The phenomenon has been discussed in the context of influencing decision-making, e.g., about personal health, election outcomes, or democratic processes (Allcott & Gentzkow, 2017; Roozenbeek et al., 2020; Tenove, 2020) with institutions still struggling to find effective means to deal with these challenges (Bennett & Livingston, 2018).

The dynamic capabilities (DCs) view has proven a valuable lens for understanding how organizations, including public institutions, adapt to challenges from a rapidly changing environment and build essential capacities to deliver value (Goh & Arenas, 2020; Pigola & da Costa, 2023; Teece et al., 1997). Responding to calls from Liu et al. (2018) and Steininger et al. (2022), amongst others, we explore how institutions can leverage information technology (IT) and develop IT-embedded DCs with the respective microfoundations to achieve their objectives, in our case by analyzing approaches to address disinformation. Recent work by Nasery et al. (2023) investigated which mechanisms the literature suggests to combat disinformation, however, they did not specify the IT-embedded DCs required for implementation. Our study uses the financial domain as research setting, where *financial fake news* (FFN) (Kogan et al., 2023; Zhi et al., 2021) are disseminated to support

* Corresponding author.
E-mail address: rath@wim.uni-koeln.de (O. Rath).

https://doi.org/10.1016/j.giq.2025.102024
Received 1 April 2024; Received in revised form 14 March 2025; Accepted 22 March 2025
Available online 11 April 2025

financial fraud schemes. FFN threatens financial market integrity by influencing investment decisions, causing stock price fluctuations (Clarke et al., 2020; Kogan et al., 2023), and posing risks of market manipulation and investor deception (Kogan et al., 2023).

Financial market (FM) institutions, such as the SEC, have already brought several cases of fraudulent schemes to courts as part of their objectives to uphold market integrity and protect consumers (Arner et al., 2022; U.S. Securities and Exchange Commission (SEC), 2023). These efforts require market surveillance techniques as well as enforcement measures, supported by established rule sets, political backing, and sufficient resources (Arner et al., 2022). However, new technological affordances, diverse media platforms, and innovative fraud methods increasingly challenge regulatory efforts to track complex disinformation-based schemes (Dupuis, Smith, & Gleason, 2023; Siering et al., 2021). This study examines how FM institutions adapt to these challenges through the use of IT-embedded dynamic capabilities.

This study seeks to advance the conceptualization of FFN, its role in fraudulent schemes, and the role of IT, derived from insights of FM institutions. Specifically, we aim to identify the IT-embedded DCs developed by financial institutions to achieve their objectives in addressing disinformation campaigns. Accordingly, we pose the following research questions:

- ***RQ1:*** *How are financial fake news characterized?*
- ***RQ2:*** *Which IT-embedded dynamic capabilities do financial market institutions apply to counter financial fake news?*
- ***RQ3:*** *Which open challenges do financial market institutions face in countering FFN schemes?*

To systematically investigate these questions, we employ a two-step qualitative approach in our research. First, we compile a dataset of 378 litigation and complaint cases issued by regulatory financial institutions and use a taxonomy development approach to investigate how FFN schemes are played out and what characterizes their nature to understand the challenges institutions are facing. Second, we collected documentation of countermeasures, strategic directions, and technological means at the hands of the institutions based on a set of 131 reports, speeches, and strategy papers that were published by international FM institutions. The second set serves as a corpus of practical experience that allows us to derive the IT-embedded DCs that these organizations developed.

Our theoretical contributions are as follows. First, we enrich disinformation and FN research by providing a taxonomy of FFN schemes, highlighting their practical characteristics and the specific challenges they pose, and supplementing existing financial fraud taxonomies (Clapham et al., 2023; Siering et al., 2017). Second, we present a framework of IT-embedded DCs used by financial institutions to combat FFN, offering a foundation to explore similar capabilities in other high-risk public domains. Third, we address a gap in DC literature by examining IT-embedded DCs in public institutions, structuring their micro-foundations and IT resources. Unlike prior research focusing on firms, our study provides an end-to-end perspective, linking FFN challenges to the DCs developed to address them using real-world empirical evidence.

Our research offers practical value for institutions, regulators, and the public. It consolidates the DCs used by FM institutions to counter disinformation, providing a practical reference for strategies to maintain market integrity and protect consumers. Regulators can use our taxonomy to assess fraud cases involving disinformation, while retail traders can gain awareness of FFN schemes' sophistication and impact. Beyond finance, our findings demonstrate how IT-enabled capabilities can help institutions fulfill mandates and meet regulatory demands, offering guidance for sectors like healthcare or politics, where information quality and regulatory compliance are critical.

2. Theoretical background

Our work builds on two main theoretical foundations: a) contemporary studies on disinformation and FN and the challenges they pose to institutions, and b) DC theory as a foundation for institutions to deliver value through timely responses to external changes.

2.1. Disinformation and fake news as challenges to public institutions

Disinformation and fake news have become a major public concern and a growing research focus over the past decade (Pérez-Escolar et al., 2023). Academic discourse on disinformation intensified following its role in the 2014 annexation of Crimea (Saurwein & Spencer-Smith, 2020) and the 2016 US election, where conspiracy theories like Pizzagate (Tandoc Jr. et al., 2021) and false news on social media may have influenced the outcome (Allcott & Gentzkow, 2017). This spurred further research on the impact of disinformation on events such as the Brexit vote and national elections, raising concerns about the role of social media in undermining democratic processes (Jungherr & Schroeder, 2021; Tenove, 2020). Researchers highlight growing societal polarization fueled by social media discussions on political decisions and social issues (Kushwaha et al., 2022). In healthcare, disinformation campaigns around COVID-19 affected vaccination willingness (Roozenbeek et al., 2020). Misleading information also creates significant cybersecurity and performance risks for businesses (Petratos, 2021).

According to Khan et al. (2022), false information can be classified into two aspects: its truthfulness (facticity) and the creator's intent. This leads to three types of false information: a) *misinformation*: propositional content of signs that misrepresents the state of the world without the intention to deceive, b) *disinformation*: propositional content of signs that misrepresents the state of the world with the intention to deceive, which is the focus of our work, and c) *malinformation*: propositional content of signs that truthfully represents the state of the world with the intention to deceive.

Information manipulation theory (IMT) (McCornack, 1992) explains how disinformation and fake news (FN) are used by fraudsters to manipulate audiences. IMT identifies four principles of deceptive communication: a) exaggerating or understating information to distort the truth; b) altering the quality of information or presenting falsehoods; c) taking information out of context; and d) using ambiguity to confuse readers. Saurwein and Spencer-Smith (2020) describe online disinformation as a socio-technical assemblage involving producers, sharers, social media users, companies, and platforms. The interplay of these elements creates significant challenges for institutions, with researchers warning that an order of disinformation is developing (Bennett & Livingston, 2018).

The term *Fake News* is understood differently as a scientific construct. First, the definition of news has evolved with new platforms, media formats, content, and contexts. Traditional news values have broadened to reflect this spectrum (Tandoc Jr. et al., 2021). Some studies adopt a broad definition, such as "any story or claim with an assertion in it" (Vosoughi et al., 2018, p.1), to expand the view on this construct. Second, the application of FN varies across disciplines and does not fully address the challenges of false information in media and society (Khan et al., 2022). Some scholars reject the term due to its conceptual ambiguity (Khan et al., 2022) and its misuse in public discourse to discredit news sources (Vosoughi et al., 2018).

We align with Vosoughi et al. (2018) in supporting FN as a scientific construct due to its political salience, particularly in public domain research. To enhance clarity for our research, we define FN as intentionally false or misleading information (disinformation) in digital messages actively designed, promoted, and distributed to deceive and cause harm, building on IS researchers (George et al., 2021; Khan et al., 2022) and institutional guidelines (High Level Group on Fake News and Online Disinformation (HLEG), 2018).

2.2. IT-embedded dynamic capabilities

Given the increasing complexity of disinformation campaigns, institutions require structured approaches to detect, analyze, and mitigate FFN. Dynamic capabilities theory, rooted in the resource-based view, is a key business and IS framework explaining how firms achieve sustainable competitive advantage (Eisenhardt & Martin, 2000; Teece et al., 1997). According to Teece et al., a "firm's dynamic capabilities govern how it integrates, builds, and reconfigures internal and external competencies to address changing business environments" (Teece et al., 2016, p. 9). DCs enable organizations to sense opportunities and threats, mobilize resources to achieve strategic objectives (seizing), and transform internally and externally. Microfoundations, the underlying routines and competencies that shape an organization's dynamic capabilities, explicate how organizations leverage their resources to build their dynamic capabilities (Teece, 2007).

Technological advancements have increased the importance of IT-related resources, making them critical for adapting to dynamic environments, such as by enhancing organizational agility (Teece et al., 2016). Conceptualizations of DCs and IT's role vary widely, as Steininger et al. (2022) highlight in a critical review. They propose a framework for DCs in IS research, emphasizing that DC constructs should a) involve sensing, seizing, or transforming capacities, b) distinguish IT-embedded from non-IT-embedded DCs, and c) separate cause and effect. Our study follows their suggested path, uncovering IT-embedded DCs in financial institutions distinguishing between sensing, seizing, and transforming capacities.

IT plays a key role in enabling and shaping DCs, with IS research identifying four primary roles: as an enabler, embedded within DCs, a contextual element, and an outcome (Steininger et al., 2022). IT is often viewed as an enabler, comprising assets (e.g., IT infrastructure) or competencies (e.g., IT-leveraging capabilities) that support DC development and enhance performance (Wamba et al., 2017; Zardini et al., 2016). This "tool view" focuses on IT's role in improving productivity and information processing. Some studies integrate IT into DCs, emphasizing its interplay with people and processes (e.g., Lim et al., 2011), while others analyze IT as a context or outcome, such as in digital transformation (Koch, 2010). Although the "tool view" dominates, recent research increasingly highlights IT's embedded role in driving organizational agility and adaptability.

3. Related literature

Our work spans established research areas, and we identified several related studies. This section discusses key papers that contextualize our study, focusing on financial markets, approaches to combating disinformation, and organizational DCs.

3.1. Fake news in the context of financial markets

FMs are complex systems, subject to constant change and external shocks (Münnix et al., 2012). The widely accepted Office of the Comptroller of the Currency (OCC) definition describes FMs as platforms or systems enabling buyers and sellers to trade financial instruments such as bonds, equities, currencies, and derivatives (Office of the Comptroller of the Currency (OCC), 2023). Regulatory objectives of FM institutions include market stability, consumer protection, and market integrity (Arner et al., 2022), with the latter two being critical for addressing FFN-based fraud, as such schemes typically target individuals and specific market segments rather than overall stability. Consumer protection seeks to safeguard consumers from overreach by financial institutions, drive increased confidence in the financial system, and reduce financial crime. Market integrity emphasizes the elimination of market abuse and fraudulent activities, non-discriminatory access, transparency, and accurate information of the FM (Austin, 2016).

The financial sector operates under established rules, supervision, and institutions (Arner et al., 2022). The largest stock exchanges are located in the US, China, Europe, Japan, and India (World Federation of Exchanges (WFE), 2024). Global bodies such as the International Organization of Securities Commissions (IOSCO) recommend regulations that local regulators implement, often inconsistently (Arner et al., 2017). The regulatory framework, as outlined publicly, is highly complex, and its implementation into national law can vary significantly (Arner et al., 2017). To address this, the European Union aims for more harmonized rules by establishing the European Securities and Markets Authority (ESMA) as a supervisory entity (European Security and Markets Authority (ESMA), 2024).

While FN have received significant attention, the specific domain of financial fake news remains underexplored (Fong, 2021). FFN refer to fabricated or misleading financial information, with serious implications for investors, market integrity, and public trust (Fong, 2021). Like general FN, FFN aim to deceive, but these messages specifically manipulates financial data, market information, or company reputations. Prior studies highlight examples such as false rumors about mergers, regulatory changes, or financial performance (Kogan et al., 2023; Siering, 2019), but a comprehensive conceptualization considering its creation and distribution is still lacking. FFN can significantly impact markets: Fong (2021) shows its influence on investor decision-making, while Clarke et al. (2020) demonstrate its effects on investor attention and market reactions.

The digital era has transformed finance but introduced challenges to market integrity. FM institutions must adopt digital expertise, enhance analytical skills, and use innovative methods to maintain trust and information reliability (Siering et al., 2017). Aitken et al. (2015) found that transparent exchange trading rules and concealed surveillance mechanisms effectively protect market integrity against manipulation and insider trading.

3.2. Approaches to combat disinformation and fake news

The growing threat of disinformation and FN has prompted public institutions and researchers across disciplines to evaluate strategies and technologies to prevent, detect, and mitigate such schemes (Nasery et al., 2023; Tenove, 2020; Zhang & Ghorbani, 2020). Tenove (2020) critically analyzes policy responses in national security, electoral, and media regulation, highlighting the need for clarity on a) the risks being addressed and b) the appropriateness of measures to protect threatened normative goods. Regulators need to find a right and justifiable balance between protecting free speech and the risks of inaction, as well as empowering institutions whilst securing this power against misuse. Nasery et al. (2023) propose a four-stage framework to combat FN: a) deterrence through passive measures, b) prevention via active measures to stop FN spread, c) detection, and d) mitigation to reduce harm through information campaigns and platform interventions. This framework informs the design of IT-embedded DCs for these stages and inspires questions on regulatory effectiveness and public education in FN detection.

Methods for detecting false information online typically analyze message content, social context, and creator or user information, processed as features (Guo et al., 2020; Zhang & Ghorbani, 2020). Key trends include early detection, multi-modal data use, explanatory models for investigations, and crowd intelligence (Guo et al., 2020). In finance, studies employ machine learning and natural language processing to detect FFN. For instance, Zhi et al. (2021) propose a multi-fact CNN-LSTM model based on textual content, while Zhang and Ghorbani (2020) develop a theory-driven system using diverse features and social media patterns. While these methods show technical promise, they lack the conceptual breadth of combating FN through DCs or embedding detection into an overarching strategy.

3.3. Capabilities view in business and government research

Capabilities are mostly discussed in a business or management context but researchers have also analyzed how public sector organizations benefit from a capabilities-based view for public value creation (Wirtz et al., 2021). Recent studies provide insight into how the adoption of IS assets influences the creation of organizational capabilities in US state governments (Liu et al., 2018), what factors enable and inhibit the development of AI capabilities in government (Mikalef et al., 2022), and how AI capabilities can improve process automation, cognitive insight, and cognitive engagement for better performance of public organizations (Mikalef et al., 2023). Weber et al. (2023) followed an interpretivist research approach and analyzed data from 25 expert interviews in the field of artificial intelligence to identify the organizational capabilities required for successful AI implementation.

Van Noordt and Tangi (2023) analyzed 15 case studies from public administrations on how they acquire AI capabilities and how this relates to the creation of public value. The authors find that, whilst the need and ambition to build AI capabilities is widely accepted, these institutions face challenges in the form of advancing from legacy structure, balancing the build-up of own in-house expertise and relying on external partners, as well as advancing promising initiatives into live operations. IS researchers Pigola and da Costa (2023) derived DCs from case studies in the area of cybersecurity intelligence. The authors applied a qualitative meta-synthesis method and provide a structural reference framework for doing, enabling, improving, and managing cybersecurity.

Pang et al. (2014) conceptualize five generic capabilities enabled by IT resources in public organizations. These capabilities are deeply interconnected and arise from IT resources such as digitized administrative processes, public intelligence analytics, inter-organizational system integration, online public interactive interfaces, and public information dissemination. The *public service delivery capability* forms the foundation, using digitized administrative processes and analytics to improve efficiency and quality by reducing costs and increasing output. Building on this, the *public engagement capability* employs online public interactive interfaces to simplify citizen participation, fostering transparency and trust while enhancing the public's involvement in decision-making. As participation expands, *coproduction capability* becomes crucial, enabling collaboration with external organizations through integration of interorganizational systems. This supports resource sharing and joint problem-solving in areas like emergency response. To sustain these efforts, the *resource acquisition capability* uses analytics and information dissemination to secure political, financial, and public support by showcasing organizational effectiveness and responsiveness. Finally, the *innovation capability* ties these elements together, leveraging IT resources to create new public services and inspire private-sector innovation. Public intelligence and open data initiatives empower governments and external actors to develop novel solutions, ensuring adaptability in meeting evolving societal challenges.

Our research fills a gap in the literature by addressing how public institutions, particularly in the FM sector, can combat disinformation and FN that threaten public value objectives like market integrity and consumer protection. Existing studies often focus narrowly on detection or offer generalized insights (including various domains such as politics, healthcare, business), leaving a need to specify risks or align threats with necessary measures. Although the DC framework is valuable for understanding organizational adaptation, its application in the public sector remains limited. We argue that the dynamic environment FM institutions face, provide a meaningful environment for studying DCs in public sectors. We apply the lens of IT-embedded dynamic capabilities in FMs, structuring FFN-related fraudulent schemes through a taxonomy and analyzing responses from established institutions. Using empirical data, we clarify specific threats and the DCs institutions adopt to counter disinformation schemes. To our knowledge, this is the first comprehensive framework of IT-embedded DCs and microfoundations for institutions addressing disinformation, grounded in real-world financial market challenges.

4. Methodology

4.1. Research setting and design

Our two-step qualitative approach addresses the research questions by examining real-world actions to gain a deep understanding of FFN and institutional responses. Such methods are particularly suitable when investigating actions in specific real-world situations, offering the opportunity to gain a deep understanding of a phenomenon and its context (Miles & Huberman, 1994). First, we analyze FFN content and schemes using a taxonomy methodology (Nickerson et al., 2013) applied to a dataset of litigation releases from financial authorities. This helps conceptualize FFN and understand how it is used in fraudulent activities to mislead investors, the public, or institutions. Second, we use a grounded theory approach (Strauss & Corbin, 1990; Wiesche et al., 2017) to derive the IT-embedded DCs financial institutions employ against FFN. We analyze a dataset of reports, speeches, and alerts from financial authorities to identify patterns and relationships, uncovering the DCs and microfoundations enabling organizations to address FFN. Fig. 1 illustrates our approach.

Similar methodologies have been applied in IS research, such as Tilly et al. (2017), who used taxonomy development to conceptualize data quality, and George et al. (2021), combining structured literature reviews with grounded theory. This work is part of a three-year government-funded research project on disinformation in social media related to financial markets, involving researchers, financial social media analytics practitioners, and representatives of financial market authorities. The data collection was conducted by three doctoral students with research background in IS, financial markets, and disinformation, supported by a student assistant and supervised by a senior IS researcher. All five academics were involved in the iterations of the taxonomy development and the coding process to derive the IT-embedded DCs and their microfoundations. Intermediate results were shared and discussed in the project consortium for validation and further refinement until they were considered final.

4.2. Data collection

Our research team compiled a broad set of documents from multiple sources to gain broad empirical data on the FFN phenomenon and measures to cope with such disinformation.

4.2.1. Dataset 1: FFN cases

We make use of publicly available databases by the major financial institutions to conceptualize FFN. Through their websites, we can access litigation releases, complaints, or enforcement actions that we can filter based on search terms. Filings by the SEC, for example, have proven valuable in previous research in the field (Aggarwal & Wu, 2006; Siering et al., 2017). We make use of these databases to extract cases that involve our understanding of FFN. The resulting documents are verified practical cases and provide a comprehensive description of the false or misleading information that was disseminated, the entities involved, their victims, and the financial damage caused. However, not all websites provided appropriate data access and a sufficiently large number of documents in English.

To select relevant cases from the FM institutions we applied a keyword search. We selected keywords based on our research on the conceptualization of FFN: *((fake OR false OR misleading) AND (news OR content OR information OR articles) OR disinformation)*. We chose to limit our search to the past ten years to account for the rise of social media and the first debates on FN after the 2016 US elections. We further applied various search techniques, e.g., concatenation of search terms or Google site search, to maneuver the respective websites. Our selection of keywords resulted in 3872 keyword hits that qualified for further analysis.

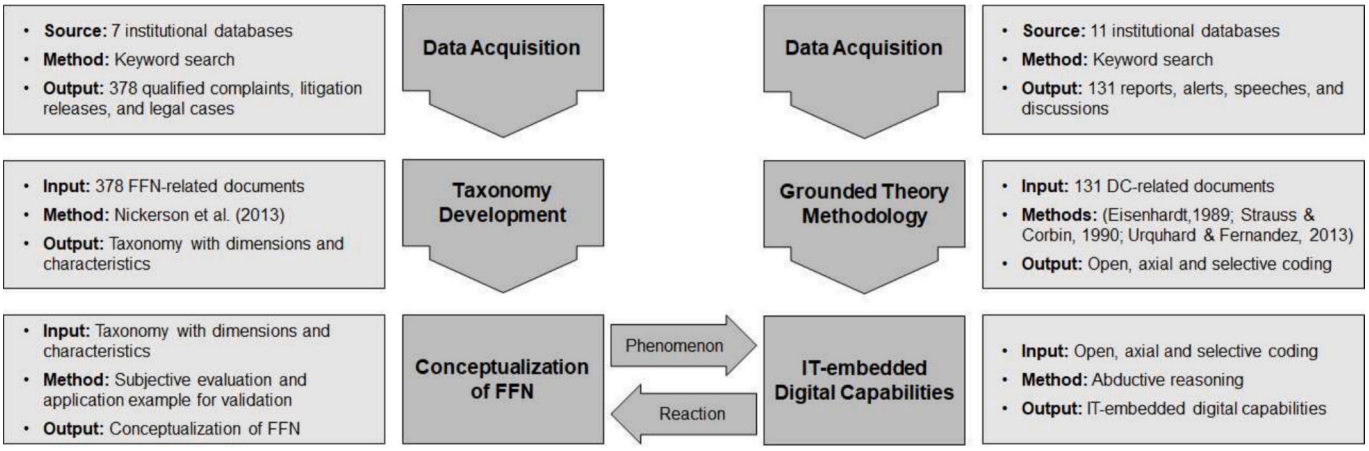


Fig. 1. Research approach.

The research team then manually screened the title and introductory information on the case or litigation release to remove duplicates and to assess if the document met our search criteria: the FFN needed to be a digital message and actively distributed via digital communication channels, the FFN needed to be used in a deceiving or fraudulent manner, and it was harmful to market integrity or consumer protection. We excluded, for example, cases where false information was provided to a regulator only. Edge cases were reviewed jointly by members of the research team to decide about their inclusion into the dataset. We ultimately included 378 documents in our dataset with most documents extracted from the SEC website. Table 1 gives an overview of the financial institutions, the keyword hits, and resulting FFN cases.

4.2.2. Dataset 2: capability documents

The compilation of our second dataset follows a similar approach but from a different angle. In addition to the national regulatory authorities we also included international institutions that focus on regulation and supervision concerning consumer protection and market integrity. We expanded our search string to reflect our focus on IT-embedded DCs: *((fake OR false OR misleading) AND (news OR content OR information OR articles) OR Disinformation AND (technology OR systems OR digital)*. Instead of retrieving litigation releases and enforcement notes, we aimed at news and regulation statements, strategy papers, regulatory actions, warnings, and public communication provided by the institutions on dealing with disinformation and FFN. Some web portals, e.g., the SEC and ESMA, allowed for filtering the categories in the document library. We sorted the documents manually for the other institutions. Our keyword search resulted in 1707 hits (Table 2).

We then screened through the results to identify documents or sections within documents that qualify for further analysis. We removed double entries, non-official communication, and opinion pieces. We further excluded legal regulatory documents and scientific work with little to no operational implications. We included documents that referred to the use of technology (IT-embedded DCs) in the context of sensing, seizing, or transforming capacities of institutions. Again, we reviewed edge cases jointly to limit individual bias. The criteria applied in the compilation of the second dataset were less formalized compared to the first dataset but that allowed for a more exploratory coding process. We acknowledge that access to information is not homogeneous across the institutions due to potential limitations in translations of relevant documents or because the reporting, issuing of press releases, or documentation is provided by other platforms.

Table 1
Relevant FFN cases per FM institution.

Institution	Region	Website	Keyword hits	FFN cases
SEC	USA	www.sec.gov	1937	251
FINRA	USA	www.finra.org	357	27
FSA	Japan	www.fsa.go.jp	334	11
FCA	UK	www.fca.org.uk	843	60
SFC	Hong Kong	www.sfc.hk	164	7
BaFin	Germany	www.bafin.de	30	4
CMA	Saudi Arabia	cma.org.sa	207	18
TOTAL			3872	378

Table 2
Documents with relevance for capability analysis per FM institution.

Institution	Region	Website	Keyword hits	Capability documents
SEC	USA	www.sec.gov	462	34
FINRA	USA	www.finra.org	82	9
FSA	Japan	www.fsa.go.jp	34	2
FCA	UK	www.fca.org.uk	183	31
SFC	Hong Kong	www.sfc.hk	28	2
BaFin	Germany	www.bafin.de	41	12
CMA	Saudi Arabia	cma.org.sa	26	1
IOSCO	Global	www.iosco.org	262	16
ESMA	EU	www.esma.europa.eu	213	7
IMF	Global	www.imf.org	263	9
WEF	Global	www.weforum.org	113	8
TOTAL			1707	131

4.3. Taxonomy development

Our sample of 378 FFN cases spans 2014–2023, with schemes lasting about three years on average. We noticed an increase in cases related to cryptocurrencies in the second half of the data but no visible rise in cases overall, as litigation can take several years. Fraud sizes ranged widely, from a few thousand to several hundred million US dollars. Large-scale frauds often involved multiple events over extended periods, such as a £230 million investment fraud executed over five years using misleading statements. We are confident that the dataset illustrates the FFN phenomenon and helps derive the major challenges for institutions. However, the data does not allow for an analysis across regions as the number of cases outside the US and UK was limited.

Our approach to taxonomy development employs the methodology proposed by Nickerson et al. (2013), which defines taxonomies as systems for groupings based on common dimensions. This methodology has been used extensively in IS research, for example, to create general taxonomies for financial market manipulations (Siering et al., 2017). Our approach provides a more rigorous methodological framework compared to an ad hoc approach to taxonomy development (Nickerson

et al., 2013). In our approach, we consider individual disinformation-driven fraud schemes as objects and use dimensions to describe their characteristic features. The disinformation techniques used in financial fraud, such as participants and effects, are considered meta-characteristics. We follow an iterative approach, where each iteration can be based on the conceptual-to-empirical or the empirical-to-conceptual approach (Nickerson et al., 2013). After each iteration, the taxonomy is derived, which consists of a set of dimensions containing a set of exclusive features. We end the approach when the objective and subjective criteria are met.

We have established objective and subjective criteria to evaluate the developed taxonomy. As objective criteria, we require that (a) the dimensions and features are mutually exclusive and collectively exhaustive to cover the diversity of FFN systems, (b) each feature appears once in an FFN scheme in our sample, (c) no dimension or characteristic has been changed in the last iteration of our development. As subjective criteria, we require the taxonomy to be concise, robust, comprehensive, extensible, and explanatory (Nickerson et al., 2013). We evaluate our approach by putting aside five randomly selected FFN cases.

4.3.1. First iteration

Using the findings of our theoretical background, we first applied the conceptual-to-empirical approach as a starting point to probe against the set of complaints and litigation cases. We derive our initial set of taxonomy dimensions from the rich work in IS on FN. Recognizing the guidance by Khan et al. (2022) to comprehensively reflect on the context of financial FN and their characteristics as a digital message, we structure our dimensions along the framework the authors provide: *Source*, *Message*, *Recipients*, *Outcomes*, *Other Digital Objects & Actors*, and *Social Media Capabilities*.

4.3.2. Second iteration

In our second iteration, we followed the empirical-to-conceptual approach starting with a random subset of 30 articles from our dataset. We applied the initial taxonomy as a guiding scheme for coding the releases by four researchers independently. Each of the researchers was assigned a random set of 6–8 articles resulting in approximately 150 pages. We used the free and open-source software Taguette (Taguette, 2023) to coordinate the coding activities. We discussed the initial results to assess if the initial taxonomy can be applied to the dataset.

In general, the research team found information on all dimensions suggested by Khan et al. (2022). Concerning the source of the message, the documents allowed us to differentiate between the type of source and the motive of the sender or creator of the FFN. Similarly, we decided to divide the message dimension into the structure of the message and its content. The same content, e.g., a text on a successful drug trial, could be presented as news or in a prospectus. We checked our end conditions and agreed that the criteria were not met at this point.

4.3.3. Third iteration

Following the second iteration, we increased our sample of articles by 50 additional articles and distributed the additional documents evenly across the research team. The results of the second iteration affected not only the characteristics, but also the dimensions of our taxonomy. Although not all litigation releases contained the messages in broad detail, most documents allowed for further content analysis. We added the four manipulation techniques from information manipulation theory (McCornack, 1992) as characteristics as they provide a sound theoretical foundation to categorize the *Type of Disinformation* that is utilized for fraudulent schemes.

Several cases in the subset span multiple years and iterations in their execution. We therefore added a *Temporal* dimension to differentiate such cases from one-time events. We also added the *Asset Type* being targeted by disinformation schemes, given that these appear to vary significantly, ranging from cryptocurrencies to securities or stocks. We found limited hints on *Other Digital Objects & Actors* as part of the dissemination of FFN, but decided to not reject this dimension yet. Since we identified the need for changes in the taxonomy, we entered the fourth iteration.

4.3.4. Fourth iteration

We then expanded our analysis to a set of 200 FFN cases. We noticed that the schemes became repetitive and that we made only small changes to characteristics within our taxonomy dimensions. We decided to deviate from the four elements of the information manipulation theory in the *Type of Disinformation* characteristics because the preparation of complaints and court cases followed a specific terminology that did not allow us to map all elements. The research team found it valuable to add the *Economic Impact* dimension to differentiate cases according to the damage caused and to add the *Fraud Type* that was supported by the FFN as this information was provided in most of the material.

In the fourth iteration, we made two changes in naming the dimensions: the *Other Digital Objects & Actions* dimension did not show the breadth of characteristics that Khan et al. (2022) covered. We decided to focus on the role of *Multipliers* like agencies, bots, and financial influencers (Haase et al., 2023) that were most important in this dimension. Additionally, we changed the *Social Media Capabilities* dimension into a *Media Channel* dimension because the unique capabilities of the platforms were rarely assessed. Based on these changes, we entered into the fifth iteration.

4.3.5. Fifth iteration

For the fifth iteration, we provided each member of the research team with the coding of another researcher with the task of reflecting on the quality of the previous results. We also screened the remaining FFN cases for additional considerations and checked how far the current results met the ending conditions. We made minor refinements to the description and naming of the characteristics to increase the precision and understanding of the terms. The research team jointly considered the taxonomy mutually exclusive and collectively exhaustive. Its characteristics occur only once per dimension, and we had no structural changes in this iteration. The research team was also confident to meet the subjective criteria we applied to our ending conditions. Therefore, we concluded the taxonomy development with our fifth iteration. The iterative taxonomy development process is illustrated in Fig. 2.

4.4. Grounded theory approach to uncover dynamic capabilities

Our second dataset provides rich insights into how financial institutions address disinformation campaigns, including, amongst others, reports, alerts and warnings, discussions, interviews, and research notes.

Using a grounded theory approach (Eisenhardt, 1989), we identify IT-embedded DCs and their microfoundations employed by regulatory institutions to counter FFN and we derive open challenges that these institutions need to address. Adopting an interpretivist stance, we systematically uncover conceptualizations embedded in the practical documents. To some degree, we take on a similar perspective as the qualitative meta-synthesis provided by Pigola and da Costa (2023), where the authors derived DCs from literature in the field as well as the work by Weber et al. (2023) that is based on practitioner interviews. Following established grounded theory practices (Strauss & Corbin, 1990; Urquhart et al., 2010), we use open, axial, and selective coding to analyze and theorize directly from the data. Guided by Urquhart and Fernández (2013), we apply an iterative process with constant comparison and joint interpretation. This multi-step method was executed collaboratively by the five researchers.

4.4.1. Open coding

The process began with open coding by examining a random sample of 20 documents distributed amongst the researchers. This stage helped us immerse ourselves in the data and gain a better understanding of the

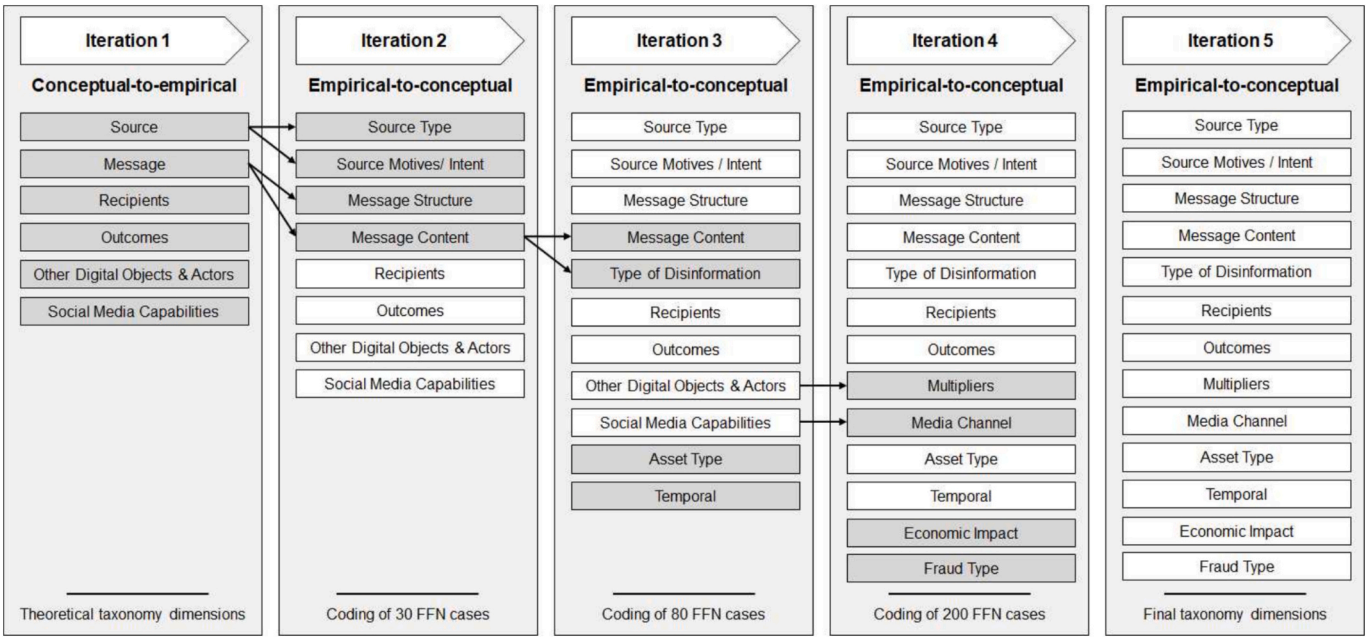


Fig. 2. Iterative taxonomy dimension development.

purpose of the documents, their structure, and the various concepts present in the documents. Codes were attributed to different statements related to, e.g., the use of technology or dealing with disinformation, again using the free and open-source software Taguette. We aimed at staying close to the source material and relied on the labels that were applied in the documents like deterrence measures or market surveillance. Our initial review revealed categories like building expert teams, knowledge sharing, and trend awareness. The institutions in our sample applied different perspectives on the issue, as expected, but we experienced several perspectives to be complementary. Our first iteration resulted in 34 codes.

After coding an increased set of randomly sampled 40 documents from our datasets, we observed a broader range of tools and software that were used by the institutions. In addition, we also aligned on coding the involvement of gatekeepers and whistleblowers in the documents. We increased the set to all 131 sample articles and started another iteration of coding. Then, we applied the constant comparative method, comparing and contrasting codes and individual documents (Strauss & Corbin, 1990). This led to discussion and code reviews mainly around the phrasing of open codes but could be resolved to result in matching codes.

4.4.2. Axial coding

We followed the Strauss and Corbin (1990) approach to axial coding after open coding to derive meaningful categories and uncover relationships between them. As suggested in the literature, we allowed for some flexibility in the coding family (Urquhart & Fernández, 2013) given that we applied the codes with care and ensured they were based on the data. Through axial coding, the study builds a conceptual framework that connects the discrete codes into a more cohesive understanding of the methods and capacities that institutions apply. Discussions in this phase were again mainly around the phrasing of individual categories. We concluded that we had saturated (Urquhart et al., 2010) across these categories, as all of the categories were already supported with the first set of 40 randomly sampled documents but got additional support by open codes during the coding of the full set of documents.

4.4.3. Selective coding

Finally, we performed selective coding by analyzing the codes in our main categories. Selective coding is critical in abstracting the data to a level where more theoretical conceptualizations can be formed (Urquhart et al., 2010). The selective coding process allowed us to identify the types of IT-embedded dynamic capabilities FM institutions employ in coping with disinformation. We further structured which underlying microfoundations support these DCs, identified the key IT resources in line with Pang et al. (2014), and documented the open challenges that emerged.

The Table 3 illustrates our coding process in exemplary passages from the documents, noting the open and axial codes that we applied to the passages and the themes that emerged from our selective coding.

5. Results

5.1. Taxonomy of FFN schemes

Based on our taxonomy development approach, we derived a taxonomy of FFN schemes comprising 13 dimensions (see Table 4), expanding on the structure provided by Khan et al. (2022). Each dimension addresses a distinct aspect of FFN, serving as a valuable tool to conceptualize the phenomenon. Two dimensions provide structure to the source of the FFN. The *Source Type* characterizes the entities responsible for the crafting of the false message and drive the dissemination. These entities include individual retail traders, individuals in leading management positions, and those with a professional finance background. The *Source Motives / Intent* dimension structures the reasons individuals engage in the dissemination of FFN.

The three dimensions that hold characteristics of the message are *Message Structure*, i.e., whether the message is presented as news or filing, or another format, *Message Content*, referring to the topic and context provided in the message, and the *Type of Disinformation*, i.e., whether the FFN contained false information, rumors, or omissions. The *Recipients* dimension categorizes the entities that are victims or targets of the FFN, including institutional and retail investors, analysts, employees, and clients. The taxonomy also considers the real-world-consequences of FFN under *Outcomes* dimension, such as embezzlement, fluctuations in asset prices, changing trading volumes, or the triggering of corporate action.

The factors enabling the broad dissemination of FFN are described in the *Multipliers* and *Media Channel* dimensions. *Multipliers* include bots,

Table 3
Exemplary illustration of the coding process.

Document text	Codings: open (underlined) and *axial (italic)*	Themes from selective coding
SEC_discussion_1: We launched the SEC Action Lookup for Individuals, or SALI, a new online search feature that enables retail investors to research whether the person trying to sell them investments has a judgment or order entered against them in an enforcement action.	Software, Investor information, Data Availability *Data Sharing*	Several themes addressed the need to have FFN-related information available and accessible for purposes of linking data internally, to exchange with other regulatory bodies, or for information towards consumers
SESC_report_2: […] the SESC routinely receives a wide range of information from investors and others[…]. The SESC also cooperates with SROs to gather a variety of information related to financial and capital markets. Based on the information, the SESC analyzes the background of individual transactions and market trends, examines transactions for suspected market misconduct, and reports to the relevant divisions in the SESC if any suspicious transactions are identified.	Linking Databases, Pattern Detection, Data Availability *Market Intelligence*, *Analytics*	The application of analytical methods to an integrated dataset across databases allowed regulators to detect fraudulent activities
IOSCO_report_6: IOSCO members should also consider ways to develop appropriate monitoring programs for the surveillance of online marketing and distribution activities, including on social media. […] capacity could include: the power to request access to content to detect illegal or misleading promotions; having regulatory channels in place to report consumer complaints for misleading and illegal promotions; and suitable evidence tracking processes in place to cope with the fast pace and changing nature of online information.	Monitoring, Data Access, Reporting Channels, Pattern Detection *Enforcement*, *Detection*, *Surveillance*	The ability to enforce rules in digital media presented an emerging scheme across institutions. The use of reporting channels for consumers and whistleblowers has been noted as highly valuable in detecting FFN schemes and deterring fraudsters.

financial influencers, promotional agencies, or (sub-)communities while *Media Channels* encompass various distribution platforms, each with a different impact on reach and dissemination speed. Additional context for FFN is provided by the dimensions *Asset Type*, *Temporal*, *Economic Impact*, and *Fraud Type*, e.g., pump-and-dump (Rath et al., 2024), allowing for the sorting of FFN schemes, for example, by jurisdiction, and setting priorities or scope of investigations.

We also report the percentage of occurrence for each characteristic to provide basic descriptive statistics of FFN schemes and aid in addressing solutions. Since FFN cases can involve multiple characteristics per dimension (e.g., the *Source Type* for a single case might include owners, underwriters, and external authors), the number of occurrences varies per dimension. Thus, we consider the percentage of occurrence per dimension to offer better guidance on dominant characteristics.

A majority of the FFN cases in our dataset involved company owners and insiders. Approximately 60 % of cases were motivated by self-benefit, although instances of concealment or serving other beneficiaries were also observed. Reports, prospectus, and news were the main characteristics identified in the *Message Structure* dimension, whereas manipulated or false information on financials and reporting data dominated the *Message Content* and *Type of Disinformation*. Video and audio play a minor role in our dataset.

Recipients of FFN messages were primarily institutional investors and traders, with significant mention of (sub)communities such as the elderly and ethnic / religious groups (9 % and 4 %, respectively). Asset price changes and embezzlement / misappropriation were the main *outcomes* of FFN schemes. External agencies and (sub-)communities often served as *Multipliers*, while websites and traditional media remained the main *Media Channel*, followed by direct communication and social media.

Besides stocks and securities, cryptocurrencies are increasingly targeted as financial instruments. The investigated cases typically spanned multiple months or years, most often causing substantial *Economic Impact*, ranging from $10 million to $100 million. Notably, approximately 9 % of FFN cases caused a massive amount of financial damage greater than $100 million. The *Fraud Type* was often characterized as securities fraud, with established types such as pump-and-dump and Ponzi schemes also frequently identified.

We evaluated our taxonomy in two ways: first, we applied the taxonomy to the five randomly selected FFN cases we put aside before the taxonomy development. As we already experienced in our fifth iteration, our taxonomy is very robust and was well suited to structure the FFN cases along its dimensions. We further found the taxonomy to be both practical and useful in mapping the cases and characterizing their unique features.

Second, we provided a subjective evaluation following the guidance provided by Nickerson et al. (2013) and also reflected on our findings with the external partners in our research group. Effective taxonomies need to be concise, as a taxonomy that is too broad in dimensions and characteristics can become arbitrary. We consider our taxonomy of 13 dimensions balanced and sufficiently concise to conceptualize the FFN phenomenon although the taxonomies by Siering et al. (2017) and Clapham et al. (2023) required fewer dimensions. The litigation cases, however, were very rich in information and had a practical need to be very precise, so we consider our taxonomy to reflect on the nature of the documents. Furthermore, we are confident our taxonomy is robust, as it allows for a clear distinction in the different FFN schemes in our dataset and a change in characteristics also leads to substantial changes in the scheme.

As our taxonomy is built on an extensive set of 378 real-world cases across multiple geographies and a solid theoretical foundation, we consider it comprehensive in covering the breadth and unique features of FFN. Concerning extensibility, we are confident that our taxonomy is flexible enough to include novel objects or dimensions. Although it is difficult to predict future FFN schemes, our taxonomy is built mainly on non-contemporary dimensions grounded in theoretical tenets that can be extended with new elements. Finally, a taxonomy should have explanatory power, i.e., a taxonomy should make it easy to understand its scope without having to describe each object in detail. We argue that there is very little FM-related knowledge required to understand the taxonomy based on the dimensions and their brief description illustrated in Table 4.

5.2. IT-embedded dynamic capabilities framework

As a result of our selective coding, where we aimed to structure the more abstract conceptualizations emerging from the data, we identified five IT-embedded DCs, *Dynamic Fraud Awareness*, *Collaborative Investigative Networking*, *Rapid Enforcement Adaption*, *Digital Communication and Education*, and *Effective and Visible Deterrence*, that we considered paramount for the financial institutions in dealing with FFN and in enabling public value creation with respect to creating operative and sustainable

Table 4
Taxonomy of FFN schemes.

Dimension	Description	Characteristics (percentage of occurrence in parentheses; $n = 378$)			
Source Type	Represents the type and role of the sender.	Owner	(22 %)	Promotion Firm	(9 %)
		Insider	(20 %)	External Author	(8 %)
		Large Shareholder	(10 %)	Underwriter	(7 %)
		Professional Trader	(10 %)	Retail Trader	(3 %)
		Broker	(10 %)	Market Maker	(1 %)
Source Motives / Intent	The reasons and objectives that motivate the dissemination of FFN.	Self-Benefit	(60 %)	Conceal Activities	(11 %)
		Serve Beneficiaries	(25 %)	Damage Asset	(4 %)
Message Structure	Refers to the structure and presentation of the message.	Reports	(25 %)	Filing	(17 %)
		Prospectus	(23 %)	Short-Message/Post	(12 %)
		News	(19 %)	Video/Audio	(4 %)
Message Content	Describes the specific content of the FFN.	Financials	(32 %)	Partnerships	(10 %)
		Reporting	(27 %)	Testimonial	(5 %)
		Breakthrough/New Business	(13 %)	Mgmt. Changes/Team	(3 %)
		Transaction	(10 %)		
Type of Disinformation	Refers to the nature of the fake news itself.	Manipulated Information	(48 %)	Omissions	(5 %)
		False Information	(44 %)	Rumors	(3 %)
Recipients	Describes the entities that receive and potentially act upon the FFN.	Institutional Investors	(36 %)	(Sub-)Community	(9 %)
		Professional Traders	(15 %)	Analysts	(6 %)
		Retail Traders	(15 %)	Ethnic/Religious Group	(4 %)
		Clients	(14 %)	Employees	(1 %)
Outcomes	Represents the actual or likely impact of the FFN scheme.	Price Change	(42 %)	Trading Volume Change	(14 %)
		Embezzlement/Misappr.	(40 %)	Corporate Action	(4 %)
Multipliers	Other digital objects or actors that multiply the dissemination of the FFN.	Agencies	(53 %)	Financial Influencers	(13 %)
		(Sub-)Communities	(30 %)	Social Bots	(4 %)
Media Channel	Relates to the medium through which the FFN is propagated.	Traditional Media	(31 %)	Social Media	(18 %)
		Websites	(26 %)	Video/Audio Platforms	(5 %)
		Direct Communication	(20 %)		
Asset Type	Refers to the financial instrument targeted by FFN.	Stocks	(41 %)	Cryptocurrencies	(11 %)
		Securities	(41 %)	Real Estate	(7 %)
Temporal	Considers the temporal diffusion of the FFN scheme.	Long-Term Scheme	(85 %)	Single Event	(15 %)
Economic Impact	Structures the impact of the scheme based on the amount of financial damage caused.	Substantial	(36 %)	Large	(27 %)
		Minor	(28 %)	Massive	(9 %)
Fraud Type	Refers to the underlying fraudulent scheme where disinformation is used.	Securities Fraud	(39 %)	Paid Promotion	(6 %)
		Pump-and-Dump	(22 %)	Pyramid Scheme	(3 %)
		Ponzi Scheme	(14 %)	Kickback Scheme	(2 %)
		Market Manipulation	(12 %)	Short Attack	(2 %)

advantages internally and providing better services externally (Wirtz et al., 2021), especially on the core mandates of consumer protection and market integrity.

Fig. 3 provides the resulting framework of inputs, microfoundations and the resulting DCs that we derived from the dataset. With respect to *sensing*, institutions focus on identifying disinformation through proactive monitoring and awareness. Given increased awareness, DCs enable to respond and act upon (potential) violations via *seizing* mechanisms. Lastly, emphasized adaptation, education and deterrence mechanisms allows FM institutions to address evolving threats via *transforming*. The framework integrates inputs, comprising technological resources as well as organizational and managerial resources, which enable the development of DCs. These inputs are operationalized through microfoundations, routines in the cooperation between institutional specialists and technology, that provide the working mechanisms required to address disinformation effectively. The framework links these activities to broader outputs, especially to deliver public value by ensuring market integrity and consumer protection. In the following, we will describe each DC, their microfoundations and key IT resources employed by FM institutions in more detail.

5.2.1. IT-embedded dynamic capabilities

Dynamic fraud awareness: Various concepts in our analysis dealt with the ability of FM institutions to become aware of developing and ongoing FFN schemes. The institutions therefore apply a broad range of techniques to sense, i.e., to get access to information that makes them aware of what is going on in the markets or on social media for different asset types. Monitoring capacity covers promotional content and retail investor behavior (IOSCO_report_7) as well as "the crypto-asset market and its interconnectedness with the wider financial system" (ESMA_strategic paper_1).

A key aspect of information collection lies in the involvement and close cooperation with gatekeepers, whistleblowers, and multipliers: "Information from market participants and investors represents candid opinions in the markets and can trigger the SESC's investigation and inspection. The SESC believes it is important to collect as much useful information from many stakeholders as possible" (SESC_report_1). Most institutions have established whistleblower systems designed to ensure

anonymity (BaFin_Report_1; FCA_alert_1) as well as reporting hotlines, chat systems, and online forms in cases where less sensitive information is shared (IOSCO_report_3). FM institutions see value in combining offline and online data, as one participant in a US SEC discussion forum illustrated regarding public awareness: "one of the perpetrators of that had 25 cars in his driveway. Probably a pretty good sign he's either doing something well or maybe something else. So those are the types of very subtle pieces of data that might help head off a retail fraud" (SEC_discussion_1).

Additionally, the institutions in our sample apply various analytical methods to identify patterns and connections in the data they receive. The use of machine-learning-based models (often discussed as AI) has increased visibly in past years as examples from BaFin and SEC illustrate: "The use of big data and artificial intelligence to combat market abuse is being expanded in order to strengthen information analysis" (BaFin_report_3); "increased use of data and data analytics to detect and investigate misconduct" (SEC_speech_3). This allows institutions to "take advantage of today's data-rich environment. The result is that the number of cases we are able to originate in-house has risen dramatically" (SEC_speech_3). The IOSCO encourages further analysis of warning signals in patterns, e.g., "[i]ncreased trading/investing activity of vulnerable retail investor population, such as retirees and new and young investors", or "[i]ncreased offerings of unlicensed financial services and products, including on a cross-border basis" (IOSCO_report_7). Evasion of regulation is a concern that influences this DC: "Regulators face the challenge of enhancing monitoring as activity shifts to new trading venues and counterparties. Trading platforms […] are structured in ways that lead them to not always fit neatly under the existing regulatory regime." (IOSCO_report_4).

Collaborative investigative networking: The seizing capacity of this DC allows institutions to quickly make use of observations and findings from national institutions or international partners and enrich its own sources of information (IOSCO_strategic paper_2). The aim is to provide and align on the same quality of information to relevant entities that are faced with an issue or fraud scheme involving FFN and to allow for an orchestrated approach in the investigation, across borders when required (IOSCO_strategic paper_2). Reports on the first appearance of a FFN, for example on a novel cryptocurrency-related promotion with unsupported claims of technological innovation, allow for tracing the origins when the news spread. A report by the German BaFin explains as follows: "Especially when investigating these types of, usually complex, cases, it is necessary to cooperate promptly and efficiently with supervisory authorities around the world in order to pool information and, if necessary, coordinate a joint approach." (BaFin_report_2). The layered global architecture of FM supervision is credited as a valuable driver for this capability.

Joint investigations of potentially fraudulent activities require a close alignment between technological and organizational processes and resources. Several tools are already in place: "Authorities should continue to use supervisory and enforcement information tools to enhance cross-border cooperation and coordination" (IOSCO_report_4), however, documents also describe the challenges to overcome in developing this DC, especially in the harmonization of technical and communications standards, jurisdiction, and the pace of enforcement (FCA_report_4). Overreach is another concern, as institutions could "move to shut down systems, erect higher digital barriers or embark on digital colonization (by monopolizing digital systems) for geopolitical ends" (WEF_report_1).

Rapid enforcement adaption: In order to act upon the insights generated from the institutions' own sensing capabilities or investigation outcomes, enforcement actions need to be "timely and adaptable" (SEC_speech_3). Institutions need to continuously adapt enforcement protocols and tools to address emerging fraud tactics as they evolve. This encompasses intervention in the trading of assets, the use of take-down systems or moderation-mechanisms on social media, but also the dynamical modification of analytics tools to address specific regulatory and fraud contexts or asset classes, e.g., in the cases of new DeFi scams or NFT-based schemes (FCA_speech_3).

In preparation for enforcement actions, SEC officials state the principle that their teams "investigate to litigate", i.e., "that we have asked the staff to conduct all investigations with litigation in mind" (SEC_speech_3). This implies the availability of sound and compelling data and the compilation of extensive case files required in pursuing legal action. With the emergence of new social media, this also requires adapting systems to store and analyze short video content instead of metadata and text bodies only for robust evidence collection.

Digital communication and education: The high number of alerts in our data sample was a key driver for the capability that encompasses general communication, public information sharing, educational efforts, and the issue of warnings through FM institutions. The institutions emphasize the broad spectrum of their channel presence which includes, amongst others, "publishing prohibited or other warning lists; newsletters; use of

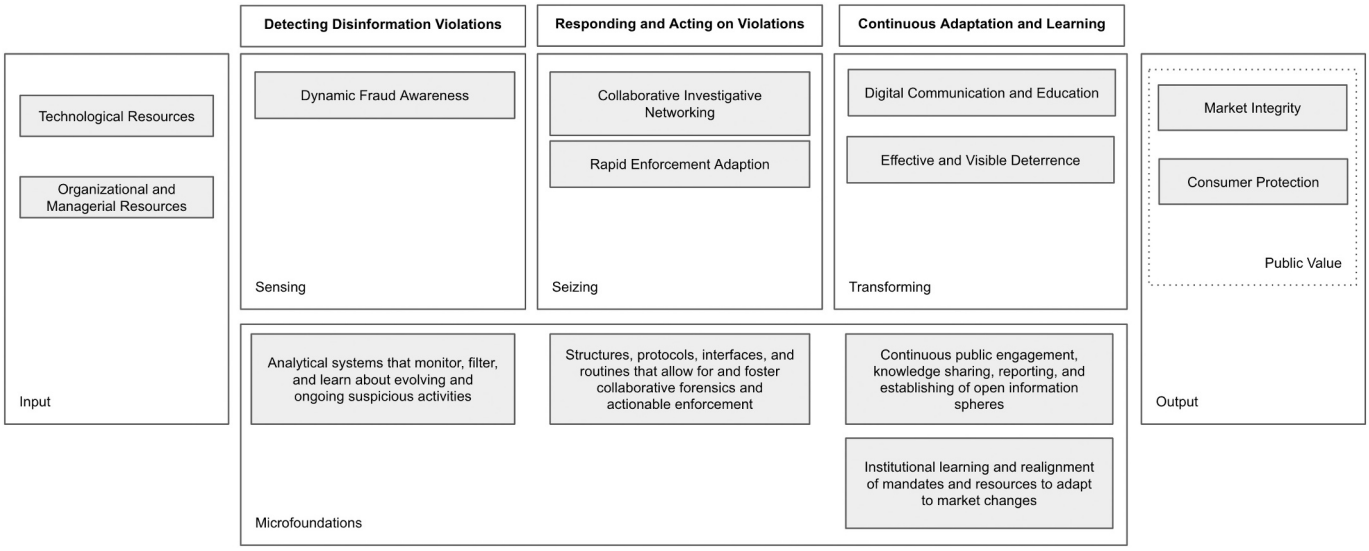


Fig. 3. IT-embedded DCs for public institutions coping with disinformation.

websites to inform investors; advertising and engaging campaigns which seek to educate investors on the warning signs of a potential scam" (IOSCO_report_3), and some authorities embark on more modern approaches with "new digital and social channels from RSS feeds to content marketing", events (fraud bingo), and educational videos (SEC_discussion_1). The DC is seen as one of the major cornerstones in building trust in both FM institutions but also in market integrity and consumer protection.

One of the key qualities of this capability lies in tailored messaging. Several documents in our sample raised the need to reflect on the vulnerability of the target audience. As we identified in our conceptualization of FFN, such campaigns targeted specific communities like the elderly, military personnel, or ethnic groups (IOSCO_report_8). This results in the need to ensure that information or alerts reach these specific communities, "[t]ailoring messaging to retail investors for different websites and social media forums" (IOSCO_report_2). The content further needs to reflect on financial education and technology literacy of their audience and campaigns can be supported by technologies to customize and automate and involve concepts like edutainment or gamification (ESA_report_1).

Financial market institutions also invest in understanding the motives and behavior of both fraudsters as well as victims to incorporate into their communication measures. Studies assessed "attitudes, understanding, motivations, and beliefs that underpin people's decisions" (FCA_report_2) of investors falling for scams. Officials warn of victim shaming to ensure that cases are brought forward and institutions can provide help (SEC_discussion_1). Education and raising awareness hence need to build on behavioral research and psychology to be most effective and "regulators should explore new ways to build investor capabilities through different forms of engagement that seek to build skills rather than just knowledge, as both aspects complement each other" which can include digital tools, short videos, fake scam websites, and broader investor education initiatives (IOSCO_report_2). The *Digital Communication and Education* capability is a strong enabler for transforming capacities as increased awareness and improved investor education have the potential to significantly reduce the need for dealing with disinformation eventually, thereby freeing up resources to build or strengthen other capabilities.

Effective and visible deterrence: As illustrated by Nasery et al. (2023), deterrence is a crucial element to combat disinformation and we observed that concept applied in practice. What characterizes this DC are major debates and perspectives on the effectiveness of deterrence measures as well as its visibility towards both audiences: actors involved in FFN schemes and the public (e.g., the SEC Action Lookup). Effectiveness comprises multiple facets. First, authorities need to make sure they can litigate cases, not just with the traces of data but also with firm legislation. Rules for false and misleading statements are usually well established in FMs: "To preserve the integrity of our markets and protect investors, the Commission is charged with promulgating and enforcing rules governing certain of the business practices of the entities we regulate" (SEC_speech_1). We observed calls for balanced and appropriate enforcement actions, as well as efforts to expand the regulatory toolbox to address disinformation more seriously. Consequences for engaging in an FFN scheme can range from financial penalties, disgorgement, affirmative steps, prohibition from practice, and admission of wrongdoing. As one official states: "I am convinced that strong enforcement has a uniquely deterrent value in white collar enforcement – sophisticated and knowledgeable market participants pay very close attention to what the SEC and the Department of Justice are doing and modify their conduct accordingly." (SEC_speech_3). The statement also underlines the aspect of visibility as a warning message to prospective fraudsters—as a statement that such schemes do not pay off—and a protective message to honest investors (IOSCO_strategic paper_2). This capability has a transformative capacity as it makes use of the legislative position and enforcement capacity of financial market authorities to discourage criminal activity by proving the power, authority and discretion of institutions, ultimately protecting markets and participants.

This DC relies on knowledge management tools and processes to support the cases that are brought forward. Strong market surveillance capacity increases the risk for detection on the side of fraudsters and therefore strengthens the deterrence capability (IOSCO_report_7). Organizations are also advised to build awareness of technology trends like robo-advisors (BaFin_report_1) and generative AI (UK_speech_6) to adapt quickly and visibly to a changing environment.

5.2.2. Microfoundations and key IT resources

We conceptualize the microfoundations supporting the DCs of FM institutions based on the guidance provided by Teece (2007). We explicate the routines we identified in the documentation which were associated with a successful build-up and functioning of the IT-embedded DCs listed above. For the sensing capacity to be of value in detecting potential FFN campaigns, organizations need appropriate infrastructure, software, and experts to utilize *analytical systems that monitor, filter, and learn about evolving and ongoing suspicious activities* (e.g., BaFin_report_3). Both DCs that respond and act on such insights heavily rely on *structures, protocols, interfaces, and routines that allow for and foster collaborative forensics and actionable enforcement*. One example lies in establishing harmonized standards for electronic case files across multiple jurisdictions for evidence management systems and the respective access rights and mandates to use the information in these files for further investigation (IOSCO_strategic paper_2). In order to transform the institutions and their market environment, institutions need to establish a culture of *continuous public engagement, knowledge sharing, reporting, and establishing of open information spheres*. This applies to targeted messaging and adequate choice of media channels, but also a relentless understanding of institutions as public servants (SEC_discussion_1). Lastly, transforming implies procedures and incentives for *institutional learning and realignment of mandates and resources to adapt to market changes*. FM institutions need to constantly evolve to keep up with novel threat scenarios, e.g., from ICO scams or deep-fakes, raising the need to understand the phenomena and make sure to have adequate countermeasures available.

In line with our second research question, we focused on the IT resources embedded in DCs through the aforementioned routines. The dominant perspectives we observed in our dataset are the tool view and the ensemble view (Steininger et al., 2022), i.e., skilled technical and non-technical experts using specific technology artifacts as an antecedent for delivering public value outcomes. We build on the framework of key technology resources for public organizations derived by Pang et al. (2014) to illustrate the mechanics, which to a large extent overlaps with the key IT resources institutions in our sample employ in dealing with challenges of disinformation. Given the highly specialized tools and processes required to take action against disinformation campaigns and enforce regulatory measures, we further added *Public Safeguarding and Enforcement* to the set of key resources. Fig. 4 illustrates the key IT resources that can be leveraged through microfoundations.

Digitized Administrative Processes build a foundation for practically all the DCs we identified and cover a broad range of fundamental systems, infrastructure and automatization to support the institutions. Organizations are advised to, for example, assure machine-readability, standardize protocols, integrate systems, automate procedures, or explore gamification elements (ESMA_report_6) and they need to ensure effective practices for technology management and cybersecurity (FINRA_report_1). Institutions further explore the use of LLMs in their software development lifecycle or generative AI for cumbersome data classification tasks (WEF_report_1).

Public Intelligence Analytics especially supports the sensing capacity of institutions. The organizations in our sample emphasize not just the value of their databases to capture external and structure internal information (e.g., suspicious activity reporting database (SEC), electronic whistleblowing system (BaFin)) but also their ability to link and

combine data sources and to handle big data characteristics (Hashem et al., 2015), e.g., the high volume of financial transactions, company fundamentals data, and social media data as well as the variety of document types. Analytical tools using AI/ML as well as monitoring and surveillance systems are also subsumed under this key IT resource. Machine-learning models, for example, are used to identify promotions that are *"likely to be misleading"* (FCA_speech_2). The German BaFin established a Data Intelligence Unit in 2021 which, amongst others, provides a supervisor cockpit as information hub (BaFin_report_4). Regulatory bodies stress the arms race between their technological efforts to monitor platforms and efforts against digital transition that allow for evading control, e.g., through new social media channels (TikTok, Discord), new or riskier products (ICOs, digital options), trading apps and robo-advisors, or emerging schemes like financial influencers (ESMA_report_6, IOSCO_report_3, BaFin_report_1).

Inter-Organizational System Integration enables collaborative investigation by facilitating coordination across institutions and sometimes jurisdictions. Important systems include information sharing platforms like the account information service provided by the BaFin which requires "credit institutions, asset management companies and payment institutions […] to store in a data file certain account master data" (BaFin_report_1). The Japanese FSC further encourages the use of AI for exchanges and regulatory bodies in information sharing with domestic and oversees institutions (FSC_release_1). An established identity and access management as well as protocols for information and escalation cascades are mentioned as crucial to build trust in such integrated systems.

Online Public Interactive Interfaces and *Public Information Dissemination* allow for organizations to effectively engage in communication, education and deterrence as transformative capacities. Interactive interfaces refer to own public facing channels like websites, social media accounts, or educational games. Preparing educational content, however, still requires significant manual effort. Information dissemination grants the public access to data and insights the institutions compiled. The SEC illustrates their use of technology resources in the example of SEC Action Lookup for Individuals (SALI), a search tool for "retail investors to research whether the person trying to sell them investments has a judgment or order entered against them in an enforcement action." (SEC_discussion_1). BrokerCheck by FINRA constitutes another example where data is enriched by an assessment through the FM institutions and legislative bodies and made available to the public.

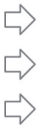
In addition to the key IT resources identified by Pang et al. (2014), coping with disinformation requires specific technology for *Public Safeguarding and Enforcement* that are distinctive from intelligence analytics tools. Related artifacts include tools to take down websites or social posts disseminating FN (IOSCO_report_3), or "mechanisms that halt trading", especially circuit breakers, that are triggered when the volatility of an asset price breaks certain predefined thresholds based usually on statistical analysis. Such actions need to be coordinated across exchanges—in part automatically—to avoid liquidity issues and evasion (ESMA_working paper_2). Highly specialized systems also include forensics tools and electronic case files for evidence management systems (IOSCO_strategic paper_2). The FCA early on successfully applied data science in this domain, e.g., clustering algorithms, topic modeling, or sentiment analysis, to detect deviations in trading patterns or uncover accounting fraud. The institute further explored data science capabilities "to create an algorithm that can scan new advertising and flag whether it is likely to be misleading." (FCA_Speech_4).

This mapping highlights how the IT resources identified by Pang et al. (2014) underpin the microfoundations and hence the actualization of our dynamic capabilities. It emphasizes the role of these resources in creating actionable, technology-enabled responses to the complex challenges of detecting and combating disinformation in financial markets. Notably, the documents we retrieved from exchanges and institutions provided only limited information on IT architecture and hardware infrastructure components.

5.3. Open challenges for coping with FFN

The taxonomy of FFN schemes (Table 4) provides a structured view of the dimensions relevant for understanding and addressing FFN. The market environment, however, is driven by continuous change through, for example, new and evolving technology, new media channels, or new financial players and products. Hence, open challenges remain in fully leveraging the IT-embedded DCs that FM institutions employ. Table 5 summarizes open challenges that emerged from our dataset.

Key IT Resources (based on Pang et al., 2014)	Definition (based on Pang et al., 2014)	Exemplary Tools and Ensembles from FM Institutions
Digitized Administrative Processes	Information systems and infrastructures that automate administrative tasks and transactional processing, along with the ability to develop and implement such systems.	Standardized protocols, automation tools, gamification elements, technology management, cybersecurity practices, data classification
Public Intelligence Analytics	Technological tools to gather information from the public and environment and the ability to analyze and derive knowledge and insights from the information.	AI/ML systems, surveillance systems, supervisor cockpit, big data analytics, data management, external data sources (e.g., whistleblower systems)
Inter-Organizational System Integration	Integrated systems and communication technologies that enable the exchange of information and intelligence with external organizations and their integration.	Information sharing platforms, digital interfaces, system integration, contact databases, information cascades and escalation procedures
Online Public Interactive Interfaces	Online venues such as websites, social media, and mobile channels and the ability to interact with stakeholders in a bilateral and real-time manner.	Websites, social media accounts, RSS feeds, blogs, interactive events, gamification, content management
Public Information Dissemination	Infrastructures and channels through which the public can access government information repositories and the ability to publish such information in an accessible way.	Fraud databases, SEC Action Lookup for Individuals (SALI), BrokerCheck (FINRA), push messages (warnings, alerts)
Public Safeguarding and Enforcement (added)	Specialized forensics and intervention systems and tools to enable investigation, litigation, and actions on emerging fraud schemes	Circuit breakers, take-down mechanisms, forensics tools, electronic case files, evidence management systems



Microfoundations

Analytical systems that monitor, filter, and learn about evolving and ongoing suspicious activities

Structures, protocols, interfaces, and routines that allow for collaborative forensics and actionable enforcement

Continuous public engagement, knowledge sharing, reporting, and establishing of open information spheres

Institutional learning and realignment of mandates and resources to adapt to market changes

Fig. 4. IT resources required for the actualization of DCs.

Dynamic Fraud Awareness is challenged by the dynamic evolution of fraud schemes. Detecting FFN in emerging formats, such as videos or deepfakes, remains an open issue, especially by making it more difficult to trace the *Source Type* of disinformation and analyze the *Message Content*. These formats leverage advancements in generative AI to create highly convincing fake content, requiring sophisticated models to identify them. Additionally, cross-cultural disinformation campaigns and external actors complicate detection efforts, due to fraudulent activities evading scrutiny. Long-term organized disinformation campaigns, the *Temporal* dimension, present detection challenges due to often subtle evolution over time. Dealing with encryption and anonymity in modern *Media Channels* and cryptocurrency *Asset Types* also pose a significant challenge to identify emerging disinformation campaigns.

Collaborative Investigative Networking, which facilitates joint efforts across institutions, is facing open challenges in overcoming privacy and regulatory barriers to data sharing. Different jurisdiction often imposes conflicting rules on data privacy, hindering *Source Type* investigations and seamless cross-border collaboration. Regulatory bodies emphasize the importance of establishing secure information-sharing protocols and engaging internet service providers (ISPs) to seize fraud. Moreover, the lack of standards, taxonomies, and definitions for incident related data creates inconsistencies in utilizing shared information. Without globally agreed-upon templates, efforts to streamline collaboration are less effective and leave data gaps during investigations.

Rapid Enforcement Adaption enables institutions to act fast against disinformation and is crucial for addressing the *Outcomes* and mitigating the *Economic Impact* of schemes. Significant challenges persist in enforcing on and seizing anonymous actors, particularly those operating through anonymous *Media Channels* or leveraging digital currencies as mentioned above. These actors exploit the anonymity provided by such technologies, making it difficult to prosecute them. Institutions face additional challenges in streamlining the shutdown process of fraudulent content, such as social media posts or websites. Social media platforms, in particular, often require to integrate with specific take-down systems. In this respective, institutions are challenged to agree upon data-sharing agreements with social media platforms for granular data (such as post views, deleted data) to enable enforcements. Evidence tracking for long-term schemes also remains a challenges, as linking fragmented activities over extended periods require robust analytical tools.

Digital Communication and Education ultimately addresses *Recipients* and victims in focusing on proactive consumer awareness. Real-time regulatory communication channels that provide fraud warnings to consumers, such as alerts on websites or mobile apps, are increasingly important. However, ensuring that these channels are accessible, and effective across demographics is challenging. In this context, institutions explore to integrate gamification and edutainment into fraud awareness campaigns, particular for younger audiences, but this field is still in its infancy and proves challenging to manage.

Effective and Visible Deterrence aims at the design of impactful deterrence mechanisms, such as automated reminders about the illegality of disinformation, which require technical infrastructure and close collaboration with platform providers. Ultimately, such measures aim to reduce the *Economic Impact* and hinder the execution of *Fraud Types*. While such mechanisms can help deter fraudsters, challenges persist in targeting those who operate on decentralized and anonymous platforms. Setting up, maintaining, and distributing fraud history databases could serve as strong deterrent, by making fraudulent behavior known, however, this challenges institutions in ensuring that data remains accurate and comprehensive.

Table 5
Mapping of DCs to open challenges.

Dynamic capability	Challenges
Dynamic Fraud Awareness	• Detecting fake news in new formats such as videos and deepfakes. • Detecting cross-cultural disinformation and external actors. • Detecting subtle long-term schemes / organized disinformation campaigns / promotions. • Detecting disinformation campaigns in encrypted chats and cryptocurrencies.
Collaborative Investigative Networking	• Establishing secure and effective information-sharing protocols for seizing online cross-border misconduct. • Managing privacy and regulatory barriers to data sharing across jurisdictions. • Establishing common standards, taxonomies, and definitions about incident information.
Rapid Enforcement Adaptation	• Trace and seize anonymous actors behind disinformation schemes for digital currencies. • Streamlining processes and technical infrastructure for shutting down fraudulent content (e.g. social media posts). • Engagements with social media platforms for data access to more granular data for proofing activities. • Evidence tracking systems and processes for long-term schemes.
Digital Communication and Education	• Digital regulatory communication channels exposed with real-time warnings for consumers. • Design digital education initiatives for risk awareness (e.g. based on social media campaigns or gamification).
Effective and Visible Deterrence	• Design impactful deterrence mechanisms, e.g. distribute automatic reminders around illegality of disinformation on digital platforms • Deterring actors on anonymous or decentralized platforms. • Setup and maintain fraud history databases and distribute across channels.

6. Discussion

Our taxonomy illustrates the diversity and complexity of FFNs schemes. This complexity underlines the challenges that financial institutions face in combating FFN, which often feature tailored, multifaceted approaches that exploit specific regulatory or technological vulnerabilities. These findings demonstrate the need for DCs that can effectively address this diversity. Unlike other public contexts, financial institutions operate in environments characterized by heightened volatility and rapid technological change, requiring them to develop dynamic capabilities to meet their public mandates. The "arms race" discussed in our data between fraudsters and regulators illustrates this dynamic, as fraudsters continuously adapt to technological advancements, requiring institutions to respond with increasingly sophisticated tools and strategies.

Our findings reveal that the challenges posed by FFN are largely consistent across jurisdictions, despite variations in the spectrum of cases observed, the fundamental issues faced by financial market regulators were comparable across regions. This suggests that FFN is a global problem that necessitates coordinated, cross-border responses. However, this alignment introduces additional challenges, particularly in ensuring data sharing and collaboration across jurisdictions with varying regulatory frameworks and privacy standards. Advanced tools, such as AI-based analytics and social media monitoring, play a pivotal role in detecting and addressing FFN but raise critical concerns about privacy and legitimacy in democracies (Königs, 2022). Automated enforcement mechanisms and cross-border data sharing, while effective, can bypass public oversight, creating tensions between the efficiency of these measures and their alignment with democratic values. This tension is compounded by what Aitken et al. (2015) describes as paradox: while advanced surveillance and deterrence mechanisms reduce the frequency of fraudulent activities, they may inadvertently encourage fraudsters to tailor schemes that exploit published loopholes. Our findings support this observation, emphasizing the need for continuous adaptation in regulatory approaches.

The reliance on IT and AI in the DCs we identified underscores the importance of explainability in AI decision-making processes (Preece, 2018). As these tools increasingly influence enforcement and regulatory decisions, ensuring their decisions are interpretable and justifiable becomes critical. While institutions have made significant progress in leveraging advanced capabilities, such as dynamic enforcement mechanisms and sophisticated analytical tools, our findings reveal that many challenges remain unresolved. These challenges span technical, ethical, and governance dimensions. Addressing these challenges will require a balanced approach that leverages technological advancements while upholding principles of fairness, transparency, and democratic accountability. Institutions must strive to not only keep pace with the evolving tactics of fraudsters but also maintain public trust by ensuring their measures align with societal values and expectations.

6.1. Theoretical contributions

Our study makes several theoretical contributions. First, we extend the growing body of knowledge on disinformation and FN by examining its characteristics in the financial domain and presenting a taxonomy of FFN schemes. This taxonomy supplements existing frameworks of financial fraud (e.g., Clapham et al., 2023; Siering et al., 2017) by highlighting the specific challenges posed by disinformation. Given the diversity and complexity of FN and FFN schemes, it is not surprising that there is no strong alignment on terms, reflecting the varied understanding and interpretations of the phenomenon across contexts. We provide conceptual clarity in line with Tenove (2020), focusing on the context in which false digital messages are disseminated, their structural characteristics, and the intent behind their creation. By reflecting on the framework proposed by Khan et al. (2022), we emphasize the importance of situating FN within its practical and institutional context. Furthermore, our structuring of message dimensions aligns with Information Manipulation Theory (McCornack, 1992) and FN detection research (Zhang & Ghorbani, 2020). However, our study was limited in exploring additional linguistic features of the *Message Content* dimension due to the lack of detailed text examples in the FFN cases, suggesting a need for further work in this area.

Second, we establish a framework of IT-embedded DCs that financial institutions employ to address FFN schemes. This framework identifies the mechanisms institutions use to sense, seize, and transform in response to these challenges and can inform future research for exploring such capabilities in other public, high-risk environments. Moreover, disinformation could be seen as a symptom of broader systemic market weaknesses, which makes the findings of our framework relevant beyond the FFN context. The identified capabilities, such as advanced surveillance and enforcement mechanisms, are applicable across a broader profile of financial fraud schemes. An important avenue for future research is to examine how institutions leverage these capabilities across other fraud contexts and whether they can be adapted or optimized for emerging threats.

Third, our research addresses a notable gap in the dynamic capabilities literature by examining IT-embedded DCs in public institutions. Unlike previous studies that have predominantly focused on firms, our work explores how public-sector institutions develop and deploy these capabilities to manage external threats like disinformation. This contribution extends existing knowledge on the role of IT in enabling DCs, particularly in dynamic environments for public value creation contexts.

Finally, our study offers an end-to-end perspective on the challenges posed by FFN schemes and the dynamic capabilities developed to address them. We systematically document the structure of FFN schemes, the institutional responses to these challenges, and the role of IT in supporting these responses, all based on evidence from a real-world context. This extend previous research often limited on certain aspects such as FN detection (Guo et al., 2020).

6.2. Practical contributions

Our research offers several practical implications for institutions addressing disinformation challenges. By providing a consolidated view of the DCs applied by financial institutions, our study serves as a valuable reference for developing strategies to manage disinformation effectively. Importantly, our research also serves to inform the public about the nature and mechanisms of FFN schemes. By offering a structured taxonomy of the diversity of FFN schemes, we provide knowledge that can help individuals better understand and recognize potential scams.

In addition, the insights from our research are relevant beyond the financial sector. The framework of IT-enabled DCs we present illustrates how institutions in other domains can leverage technology to meet their mandates and comply with regulatory requirements. Sectors such as healthcare or politics, where the accuracy and quality of information are essential, can apply similar strategies.

Finally, our taxonomy of FFN schemes has practical value in supporting the prosecution of fraud cases driven by disinformation. By systematically categorizing the characteristics and mechanisms of FFN, the taxonomy can help institutions better understand the methods used in such schemes, assess similarities and differences between cases, or monitor changes in patterns like the advance of cryptocurrency cases.

6.3. Limitations and future research

We are aware of a set of limitations in our work. First of all, the data we collected is limited publicly available litigation releases, which means it inherently excludes undetected or unreported frauds as well as cases that are still being investigated. There may also be selection bias as our sample over-represents SEC-related cases (251 of 378) and English-language reports. Additionally, disinformation tactics are very dynamic and constantly evolving, for example with the increased use of generative AI and new social media platforms like Discord and TikTok. This may result in a lack of comprehensiveness of our taxonomy and FFN cases that are not covered.

With respect to deriving the IT-embedded DCs, we assume a bias in the data to slightly overstate which efforts and technological solutions are in use as documents revealing major structural problems and backward technology would likely not be shared publicly. Hence, we approached the material with care and scepticism. The work by Steininger et al. (2022) recommends aligning DC constructs with how they are implemented and measured. Our current understanding of the DCs we identified did not yet reflect this level of analysis. The data for our analysis consists of strategy documents and reports that discuss IT from a high-level perspective. Future research could address both limitations by combining the documentation with expert interviews to assess how these DCs can be operationalized in practice.

Finally, while the taxonomy can help to configure and develop fraud detection systems for detecting disinformation schemes, certain dimensions such as *Sender Types* can ultimately prove difficult for automatic detection, as senders might act anonymously. Furthermore, our taxonomy does not provide concrete guidelines for the development of fraud detection systems, but rather guidance on which dimensions and characteristics should be considered.

7. Conclusion

In summary, the research conducted in this study develops a taxonomy of the use of disinformation in financial fraud and derives the IT-embedded DCs and underlying microfoundations that financial market institutions employ to cope with such schemes. We examined both a comprehensive set of FFN cases to structure and conceptualize the phenomenon as well as documentation on responses by authorities to provide an end-to-end view and discuss open challenges.

FFN can be differentiated by characteristics in their *Source*, *Message*,

Recipients, *Outcomes*, *Multipliers*, and *Media Channels* whereas the dimensions *Asset Type*, *Temporal*, *Economic Impact*, as well as *Fraud Type* allow for a structuring of relevance, jurisdiction and effort to prosecute. The five main IT-embedded DCs that we identified in our analysis that enable fraud awareness, deterrence, and educational efforts are based on a strong technological foundation as well as close collaboration with partners and other authorities. Our findings indicate that institutions in other domains could build on the capabilities and microfoundations that were established to combat FFN, and our findings might provide helpful insights into improving existing measures.

Declaration of generative AI and AI-assisted technologies in the writing process

During the preparation of this work, the authors used *Grammarly* and *ChatGPT* in order to improve language and readability. After using this service, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

CRediT authorship contribution statement

Oliver Rath: Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Resources, Project administration, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization. **Frederic Haase:** Writing – review & editing, Writing – original draft, Methodology, Formal analysis, Data curation, Conceptualization. **Johannes Werner Melsbach:** Writing – review & editing, Validation, Methodology, Funding acquisition, Formal analysis, Data curation, Conceptualization. **Jiarun Liu:** Writing – original draft, Visualization, Validation, Software, Formal analysis, Data curation, Conceptualization. **Detlef Schoder:** Writing – review & editing, Validation, Supervision, Resources, Funding acquisition, Conceptualization.

Declaration of competing interest

None.

Acknowledgements

We are very grateful to the editors and the review team for their invaluable guidance and support throughout the review and revision process. This work is part of the research project AFFIN funded by the German Federal Ministry of Education and Research (Grant no.: 01IS21045B).

References

Aggarwal, R. K., & Wu, G. (2006). Stock Market Manipulations. *The Journal of Business, 79*(4), 1915–1953. https://doi.org/10.1086/503652

Aitken, M., Cumming, D., & Zhan, F. (2015). Exchange trading rules, surveillance and suspected insider trading. *Journal of Corporate Finance, 34*(C), 311–330.

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of Economic Perspectives, 31*(2), 211–236.

Arner, D., Buckley, R., Charamba, K., Sergeev, A., & Zetzsche, D. (2022). Governing FinTech 4.0: BigTech, platform finance, and sustainable development. *Fordham Journal of Corporate & Financial Law, 27*, 1–72.

Arner, D. W., Barberis, J., & Buckey, R. P. (2017). FinTech, RegTech, and the reconceptualization of financial regulation. *Northwestern Journal of International Law and Business, 37*, 371–414.

Austin, J. (2016). What exactly is market integrity: An analysis of one of the core objectives of securities regulation. *The William & Mary Business Law Review, 8*, 215–240.

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.

Clapham, B., Jakobs, J., Schmidt, J., Gomber, P., & Muntermann, J. (2023). A taxonomy of violations in digital asset markets. In *ICIS 2023 proceedings* (p. 12).

Clarke, J., Chen, H., Du, D., & Hu, Y. J. (2020). Fake news, investor attention, and market reaction. *Information Systems Research, 32*(1), 35–52.

Dupuis, D., Smith, D., & Gleason, K. (2023). Old frauds with a new sauce: Digital assets and space transition. *Journal of Financial Crime, 30*(1), 205–220. https://doi.org/10.1108/JFC-11-2021-0242

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review, 14*(4), 532–550.

Eisenhardt, K. M., & Martin, J. A. (2000). Dynamic capabilities: What are they? *Strategic Management Journal, 21*(10–11), 1105–1121.

European Security and Markets Authority (ESMA). (2024). About ESMA. https://www.esma.europa.eu/about-esma.

Fong, B. (2021). Analysing the behavioural finance impact of 'fake news' phenomena on financial markets: A representative agent model and empirical validation. *Financial Innovation, 7*(1), 53.

George, J., Gerhart, N., & Torres, R. (2021). Uncovering the truth about fake news: A research model grounded in multi-disciplinary literature. *Journal of Management Information Systems, 38*(4), 1067–1094.

Goh, J., & Arenas, A. (2020). IT value creation in public sector: How IT-enabled capabilities mitigate tradeoffs in public organisations. *European Journal of Information Systems, 29*, 1–19. https://doi.org/10.1080/0960085X.2019.1708821

Goujard, C. (2024). *Europe wields new tech law to protect EU election.* Politico. https://www.politico.eu/article/europe-wields-new-tech-law-protect-eu-election/.

Guo, B., Ding, Y., Yao, L., Liang, Y., & Yu, Z. (2020). The future of false information detection on social media: New perspectives and trends. *ACM Computing Surveys, 53*(4), 1–36.

Haase, F., Rath, O., Kurka, M., & Schoder, D. (2023). Finfluencers: Opinion makers or opinion followers?. In *ECIS 2023 research papers* (p. 432).

Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. (2015). The rise of "big data" on cloud computing: Review and open research issues. *Information Systems, 47*, 98–115.

High Level Group on Fake News and Online Disinformation (HLEG). (2018). *A multi-dimensional approach to disinformation.* Luxembourg: European Commission.

Jungherr, A., & Schroeder, R. (2021). Disinformation and the structural transformations of the public arena: Addressing the actual challenges to democracy. *Social Media and Society, 7*(1).

Khan, A., Brohman, K., & Addas, S. (2022). The anatomy of 'fake news': Studying false messages as digital objects. *Journal of Information Technology, 37*(2), 122–143.

Koch, H. (2010). Developing dynamic capabilities in electronic marketplaces: A cross-case study. *The Journal of Strategic Information Systems, 19*(1), 28–38.

Kogan, S., Moskowitz, T. J., & Niessner, M. (2023). Social media and financial news manipulation. *Review of Finance, 27*(4), 1229–1268.

Königs, P. (2022). Government surveillance, privacy, and legitimacy. *Philosophy and Technology, 35*(1), 8.

Kushwaha, A. K., Kar, A. K., Roy, S. K., & Ilavarasan, P. V. (2022). Capricious opinions: A study of polarization of social media groups. *Government Information Quarterly, 39*(3).

Lazer, D. M., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., … Zittrain, J. L. (2018). The science of fake news. *Science, 359*(6380), 1094–1096.

Lim, J.-H., Stratopoulos, T. C., & Wirjanto, T. S. (2011). Path dependence of dynamic information technology capability: An empirical investigation. *Journal of Management Information Systems, 28*(3), 45–84.

Liu, Y., Armstrong, D. J., & Riemenschneider, C. (2018). The relationship between information systems (IS) assets, organizational capabilities, and IS-enabled absorptive capacity in U.S. state information technology departments. *Communications of the Association for Information Systems, 42*.

McCornack, S. A. (1992). Information manipulation theory. *Communication Monographs, 59*(1), 1–16.

Mikalef, P., Lemmer, K., Schaefer, C., Ylinen, M., Fjørtoft, S. O., Torvatn, H. Y., … Niehaves, B. (2022). Enabling AI capabilities in government agencies: A study of determinants for European municipalities. *Government Information Quarterly, 39*(4).

Mikalef, P., Lemmer, K., Schaefer, C., Ylinen, M., Fjørtoft, S. O., Torvatn, H. Y., … Niehaves, B. (2023). Examining how AI capabilities can foster organizational performance in public organizations. *Government Information Quarterly, 40*(2).

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook* (2nd ed.). Sage Publications, Inc.

Münnix, M. C., Shimada, T., Schäfer, R., Leyvraz, F., Seligman, T. H., Guhr, T., & Stanley, H. E. (2012). Identifying states of a financial market. *Scientific Reports, 2*(1), 644.

Nasery, M., Turel, O., & Yuan, Y. (2023). Combating fake news on social media: A framework, review, and future opportunities. *Communications of the Association for Information Systems, 53*(1), 9.

Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. *European Journal of Information Systems, 22*(3), 336–359.

Office of the Comptroller of the Currency (OCC). (2023). Financial market. https://www.occ.treas.gov/topics/supervision-and-examination/capital-markets/financial-markets/index-financial-markets.html/.

Pang, M.-S., Lee, G., & DeLone, W. H. (2014). IT resources, organizational capabilities, and value creation in public-sector organizations: A public-value management perspective. *Journal of Information Technology, 29*(3), 187–205. https://doi.org/10.1057/jit.2014.2

Pérez-Escolar, M., Lilleker, D., & Tapia-Frade, A. (2023). A systematic literature review of the phenomenon of disinformation and misinformation. *Media and Communication, 11*(2), 76–87.

Petratos, P. N. (2021). Misinformation, disinformation, and fake news: Cyber risks to business. *Business Horizons, 64*(6), 763–774.

Pigola, A., & da Costa, P. R. (2023). Dynamic capabilities in cybersecurity intelligence: A meta-synthesis to enhance protection against cyber threats. *Communications of the Association for Information Systems, 53*, 1099–1135.
Preece, A. (2018). Asking 'Why' in AI: Explainability of intelligent systems–perspectives and challenges. *Intelligent Systems in Accounting, Finance and Management, 25*(2), 63–72.
Rath, O., Haase, F., Celig, T., Melsbach, J., & Schoder, D. (2024). Profiling cryptocurrency pump and dump schemes in DeFi: A chain-level analysis of coins and participants. In *ECIS 2024 proceedings* (p. 9).
Roozenbeek, J., Schneider, C. R., Dryhurst, S., Kerr, J., Freeman, A. L. J., Recchia, G., … van der Linden, S. (2020). Susceptibility to misinformation about COVID-19 around the world. *Royal Society Open Science, 7*(10).
Saurwein, F., & Spencer-Smith, C. (2020). Combating disinformation on social media: Multilevel governance and distributed accountability in Europe. *Digital Journalism, 8*(6), 820–841.
Sellman, M. (2024). *AI deepfakes of Prince William and Keir Starmer used to sell scam*. The Times. https://www.thetimes.com/uk/technology-uk/article/ai-deepfakes-prince-william-keir-starmer-financial-scam-cryptocurrency-qgxjbj0rc.
Siering, M. (2019). The economics of stock touting during internet-based pump and dump campaigns. *Information Systems Journal, 29*(2), 456–483.
Siering, M., Clapham, B., Engel, O., & Gomber, P. (2017). A taxonomy of financial market manipulations: Establishing trust and market integrity in the financialized economy through automated fraud detection. *Journal of Information Technology, 32*(3), 251–269.
Siering, M., Muntermann, J., & Grčar, M. (2021). Design principles for robust fraud detection: The case of stock market manipulations. *Journal of the Association for Information Systems, 22*(1), 156–178.
Steininger, D., Mikalef, P., Pateli, A., & Ortiz de Guinea, A. (2022). Dynamic capabilities in information systems research: A critical review, synthesis of current knowledge, and recommendations for future research. *Journal of the Association for Information Systems, 23*(2), 447–490.
Strauss, A., & Corbin, J. M. (1990). *Basics of qualitative research: Grounded theory procedures and techniques*. Sage Publications, Inc.
Taguette. (2023). About Taguette. https://www.taguette.org/about.html.
Tandoc, E. C., Jr., Thomas, R. J., & Bishop, L. (2021). What is (fake) news? Analyzing news values (and more) in fake stories. *Media and Communication, 9*(1), 110–119.
Teece, D., Peteraf, M., & Leih, S. (2016). Dynamic capabilities and organizational agility: Risk, uncertainty, and strategy in the innovation economy. *California Management Review, 58*(4), 13–35.
Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of enterprise performance. *Strategic Management Journal, 28*(13), 1319–1350.
Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal, 18*(7), 509–533.
Tenove, C. (2020). Protecting democracy from disinformation: Normative threats and policy responses. *The International Journal of Press/Politics, 25*(3), 517–537.
Tilly, R., Posegga, O., Fischbach, K., & Schoder, D. (2017). Towards a conceptualization of data and information quality in social information systems. *Business & Information Systems Engineering, 59*, 3–21.
U.S. Securities and Exchange Commission (SEC). (2022). SEC charges company and former CEO with misleading investors about sale of Covid-19 test kits. https://www.sec.gov/newsroom/press-releases/2022-94.
U.S. Securities and Exchange Commission (SEC). (2023). Litigation release no. 25733. https://www.sec.gov/enforcement-litigation/litigation-releases/lr-25733.
U.S. Securities and Exchange Commission Investor.gov (SEC). (2022). Watch out for fake COVID-19 claims when investing – investor alert. https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/watch-out-fake-covid-19-claims-when-investing-investor-alert.
Urquhart, C., & Fernández, W. (2013). Using grounded theory method in information systems: The researcher as blank slate and other myths. *Journal of Information Technology, 28*, 224–236.
Urquhart, C., Lehmann, H., & Myers, M. D. (2010). Putting the 'theory' back into grounded theory: Guidelines for grounded theory studies in information systems. *Information Systems Journal, 20*(4), 357–381.
Van Noordt, C., & Tangi, L. (2023). The dynamics of AI capability and its influence on public value creation of AI within public administration. *Government Information Quarterly, 40*(4).
Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science, 359*(6380), 1146–1151.
Wamba, S. F., Gunasekaran, A., Akter, S., Ren, S. J., Dubey, R., & Childe, S. J. (2017). Big data analytics and firm performance: Effects of dynamic capabilities. *Journal of Business Research, 70*(C), 356–365.
Weber, M., Engert, M., Schaffer, N., Weking, J., & Krcmar, H. (2023). Organizational capabilities for AI implementation—Coping with inscrutability and data dependency in AI. *Information Systems Frontiers, 25*(4), 1549–1569.
Wiesche, M., Jurisch, M. C., Yetton, P. W., & Krcmar, H. (2017). Grounded theory methodology in information systems research. *MIS Quarterly, 41*(3), 685–701.
Wirtz, B., Langer, P., & Schmidt, F. (2021). Digital government: Business model development for public value creation - A dynamic capabilities based framework. *Public Administration Quarterly, 45*(3), 232–255.
World Federation of Exchanges (WFE). (2024). Market statistics - October 2023. https://focus.world-exchanges.org/issue/october-2023/market-statistics.
Zardini, A., Rossignoli, C., & Ricciardi, F. (2016). A bottom-up path for IT management success: From infrastructure quality to competitive excellence. *Journal of Business Research, 69*(5), 1747–1752.
Zhang, X., & Ghorbani, A. A. (2020). An overview of online fake news: Characterization, detection, and discussion. *Information Processing & Management, 57*(2).
Zhi, X., Xue, L., Zhi, W., Li, Z., Zhao, B., Wang, Y., & Shen, Z. (2021). Financial fake news detection with multi fact CNN-LSTM model. In *2021 IEEE 4th international conference on electronics technology* (pp. 1338–1341).
Zhou, X., & Zafarani, R. (2020). A survey of fake news: Fundamental theories, detection methods, and opportunities. *ACM Computing Surveys, 53*(5), 1–40.

Oliver Rath is a PhD student in Information Systems at the Cologne Institute for Information Systems (CIIS) at the University of Cologne, focusing on qualitative and quantitative research on the use of technology in the domain of financial markets, e.g., in the area of financial fraud and regulation, in the application of machine-learning models to financial documents and statements, or in the analysis of news and social media communication.

Frederic Haase is a PhD student in Information Systems at the Cologne Institute for Information Systems (CIIS) at the University of Cologne. His research focuses on the intersections of machine learning, data science, and their applications in finance. His academic contributions include analyses on financial social media, the role of influencers in finance, and financial fraud in the digital age.

JohannesWerner Melsbach is a PhD student in Information Systems at the Cologne Institute for Information Systems (CIIS) at the University of Cologne. His research covers the application of machine-learning methods for document classification as well as the use of language models in various domains.

Jiarun Liu is a research assistant at the Cologne Institute for Information Systems (CIIS) at the University of Cologne since 2023. He studies Information Systems (M. Sc.) at the University of Cologne. His scientific work focuses on the technological implementation of machine-learning models to research in the financial markets.

Detlef Schoder is a Chaired Professor for Information Systems and Information Management and Founding Director of the Cologne Institute for Information Systems (CIIS) at the University of Cologne, Germany. He was appointed reviewer to the German Parliament's Lower House for e-Commerce issues and was consultant to the European Commission. He is one of three elected academic auditors of the German Research Foundation (DFG), Germany's biggest science foundation. He was Visiting Scholar at Stanford University, University of California at Berkeley, and MIT where he established research collaboration which still continues.