RESEARCH REPORT

TECHNOLOGICAL AND ECONOMIC THREATS TO THE U.S. FINANCIAL SYSTEM

AN INITIAL ASSESSMENT OF GROWING RISKS

TOBIAS SYTSMA, JAMES V. MARRONE, ANTON SHENK,
GABRIEL LEONARD, LYDIA GREK, JOSHUA STEIER

RAND

For more information on this publication, visit **www.rand.org/t/RRA2533-1-v2**.

ABOUT RAND

RAND is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. To learn more about RAND, visit www.rand.org.

RESEARCH INTEGRITY

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behavior. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/research-integrity.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif.
© 2024 RAND Corporation
RAND® is a registered trademark.

Cover: steinphoto/Getty Images, Sevenoclockb/Adobe Stock, monsitj/Adobe Stock.

LIMITED PRINT AND ELECTRONIC DISTRIBUTION RIGHTS

This publication and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited; linking directly to its webpage on rand.org is encouraged. Permission is required from RAND to reproduce, or reuse in another form, any of its research products for commercial purposes. For information on reprint and reuse permissions, please visit www.rand.org/pubs/permissions.

ABOUT THIS REPORT

The resilience and stability of the U.S. financial system is critical to economic prosperity. However, the rapid pace of technological and geopolitical change introduces new potential threats that must be monitored and assessed. This report explores emerging and understudied threats to the financial system, focusing on risks from social media, advances in artificial intelligence, and from the changing role of economic statecraft in geopolitics.

Drawing on historical examples, the economic literature, and discussions with subject-matter experts, we assess the potential costs and likelihood of four threats: attacks on financial trading models, bond dumping by foreign holders of U.S. debt, using deepfakes to spread misinformation, and memetic engineering to manipulate beliefs and behaviors. Our analysis suggests that these threats pose a limited near-term risk of significant economic damage because of the interconnectivity of global finance and existing safeguards. However, the gradual erosion of financial resilience and institutional trust over time could make attacks more impactful.

The research reported here was completed in January 2024 and underwent security review with the sponsor and the Defense Office of Prepublication and Security Review before public release.

RAND NATIONAL SECURITY RESEARCH DIVISION

This research was conducted within the International Security and Defense Policy Program of the RAND National Security Research Division (NSRD), which operates the RAND National Defense Research Institute (NDRI), a federally funded research and development center (FFRDC) sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense intelligence enterprise. This research was made possible by NDRI exploratory research funding that was provided through the FFRDC contract and approved by NDRI's primary sponsor.

For more information on the RAND International Security and Defense Policy Program, see http://www.rand.org/nsrd/isdp or contact the director (contact information is provided on the webpage).

ACKNOWLEDGMENTS

The research team thanks our RAND colleagues, Barry Pavel, Mike Spirtas, and Jim Mitre, for their support and advice throughout this project. We are also grateful to the subject-matter experts who provided critical insight for this project through informational interviews. Danielle Schlang of RAND's Survey Research Group provided critical advice on scoping our focus groups, and Edmund Luzine provided critical advice on scoping the analysis. Finally, our reviewers, Daniel Egel at RAND and Herbert Lin at Stanford University, provided invaluable comments that greatly improved this report.

CONTENTS

About This Report III

Tables V

Key Findings VI

Technological and Economic Threats to the U.S. Financial System:
An Initial Assessment of Growing Risks 1

- Methods Used to Identify Threats 1
- Threat 1: Attacks on Models 4
- Threat 2: Bond Dumping 8
- Threat 3: Deepfakes 12
- Threat 4: Memetic Engineering 16
- Crosscutting Cost and Likelihood Considerations 20
- Conclusion 24

Abbreviations 28

Notes 29

References 33

TABLES

Table 1. Threat Objectives, Targets, and Methods 3

Table 2. Summary of Cost and Likelihood Factors 22

KEY FINDINGS

- Emerging threats to U.S. financial markets—such as attacks on artificial intelligence (AI)–enabled financial models, bond dumping, deepfakes, and memetic engineering—pose a limited risk of significant economic damage because of the high costs of such attacks to adversaries and existing market safeguards.
- However, risks may increase because of geopolitical tensions and advancing technological capabilities that alter adversaries' cost–benefit calculations.
- The most significant threat is not an abrupt event, akin to a "financial 9/11," but rather a slow and steady process, akin to "financial climate change." This phenomenon could occur when disinformation or misinformation diminishes public trust in markets, consequently complicating the distinction between reality and fabrication and thereby escalating market volatility.
- To address evolving threats, regular economic wargames that simulate and assess financial vulnerabilities should be implemented. These exercises would identify weaknesses and shape proactive countermeasures. Previous research has proposed an "Economic Joint Chiefs" framework, which could enhance these wargames by providing a dedicated structure and centralized expertise for their coordination and analysis.
- Data privacy regulations could limit the threat posed by AI-augmented disinformation campaigns. Regulations would make it harder for malicious actors to collect detailed data that could be used to create and disseminate highly customized messages to influence individual behavior.

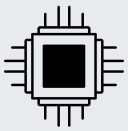
TECHNOLOGICAL AND ECONOMIC THREATS TO THE U.S. FINANCIAL SYSTEM:

AN INITIAL ASSESSMENT OF GROWING RISKS

This report provides an exploratory assessment of foreign threats to the U.S. financial system, focusing on emerging risks posed by artificial intelligence (AI), social media, and changes in the geopolitical landscape. Specifically, we study attacks on financial trading models, bond dumping, deepfakes, and memetic engineering. These threats were selected based on discussions with focus groups and subject-matter experts, as well as a detailed literature review. The box on this page summarizes the risks posed by each threat, as well as our primary methods of analysis. For each threat, we discuss prior similar events (to the extent they exist), the potential economic costs of an attack, and factors that contribute to the likelihood of an attack.

This report is meant to be an initial assessment of these threats with the aim of informing policymakers, financial institutions, and relevant stakeholders on the emerging risks and the possible courses of action to enhance the resilience of the U.S. financial system.

THREAT SCENARIOS STUDIED IN THIS REPORT



Attacks on Financial Trading Models: Algorithmic trading accounts for a large share of total trading on U.S. exchanges. This creates risks if adversaries can manipulate or disrupt algorithms or the data they use. We assess potential impacts of techniques, such as adversarial attacks and data poisoning, on neural networks used in trading.

Bond Dumping: Foreign countries hold more than $7 trillion in U.S. bonds, which—if dumped rapidly—could have the potential to roil markets. We model potential economic costs using historical cases, such as China's bond sales.

Deepfakes: Advances in AI have made it easier to generate fake images, videos, and text. Deepfakes could be used to spread misinformation and undermine trust in financial institutions. We examine historical cases in which fabricated content has moved markets.

Memetic Engineering: Memetic engineering is the process of creating and spreading memes to achieve a specific outcome. Adversaries could harness AI tools to craft viral ideas or memes that manipulate beliefs and behaviors. We examine how "meme stocks" influence broader market dynamics.

METHODS USED TO IDENTIFY THREATS

Our goal was to focus on threats to the U.S. financial system that are new, poorly understood, or for which the risks might be changing because of recent technological and geopolitical events. To identify relevant and emerging threats, we first developed a framework to describe *all* threats. We started by conducting an environmental scan of the literature. There is a large literature on financial threats that spans the risks posed by cyberattacks,[1] deepfakes,[2] cloud computing,[3] physical attacks,[4] and economic statecraft.[5] The environmental scan yielded a number of threat scenarios that had been described or assessed by scholars, industry groups, or the government.

Informed by the environmental scan, the overall framework consisted of broad threat categories and subcategories (examples of which are included in parentheses): cyberattacks (hacking, attacking algorithms and models), physical attacks (kinetic attacks, espionage, theft of assets), market

manipulation (counterfeiting currency, bond dumping), economic statecraft (tariffs, sanctions), and information operations (through social media, synthetic media).

Next, we held focus groups with RAND experts, as well as external conversations with experts in academia, industry, and government. We presented experts with several categories of threats and asked them to comment on which threats they saw as most relevant to the question of financial-sector vulnerability.

During our discussions, several primary threat vectors emerged. Nearly all experts agreed that information operations were likely to be a significant threat and that emerging AI capabilities lower the cost of carrying out such an attack. However, some experts had different concepts of information operations in a financial setting. To some, the likely method of attack was the spread of deepfake material broadcast through social media platforms. To others, the primary concern was *memetic engineering*, which is a more focused attack of ideas that may or may not involve the use of deepfakes. Several experts offered recent events, such as the collapse of Silicon Valley Bank (SVB) and the GameStop short squeeze,[6] as evidence that social media is likely to play a role in propagating deepfakes and memetic engineering attacks into the financial sector.

Cyberattacks were deemed to be a relevant threat as well, and the growing use of AI and machine learning (ML) by financial institutions was noted as a potential vulnerability. Experts noted the potential for manipulating data that feed into financial algorithms and suggested that this could be a relevant vector of attack. They considered the consequences of these vulnerabilities in a financial setting to be an important and unresolved economic question.

In addition to these cyber- and AI-related threats, we included bond dumping in the analysis—that is, the deliberate sell-off of U.S. Treasury bonds to wreak market havoc. Although experts and focus group participants downplayed concerns about market manipulation, they noted that bond dumping has been arising more often in public commentary and in their conversations with policymakers. This uptick was attributed to the changing geopolitical relationship between the United States and China. Therefore, we deemed bond dumping worthy of separate focus.

Other threats, such as physical attacks, were believed to cause only localized damage, and were better understood and surveilled than AI-related

threats.[7] Besides bond dumping, other economic statecraft measures, such as tariffs and sanctions, were deemed to be outside the scope of this project because they are traditional tools of international economic interaction and have been studied extensively.[8]

Synthesizing our discussions with subject-matter experts, we identified four unique threats: attacks on models, bond dumping, deepfakes, and memetic engineering. Table 1 displays the four threats, their objectives, primary targets, and methods.

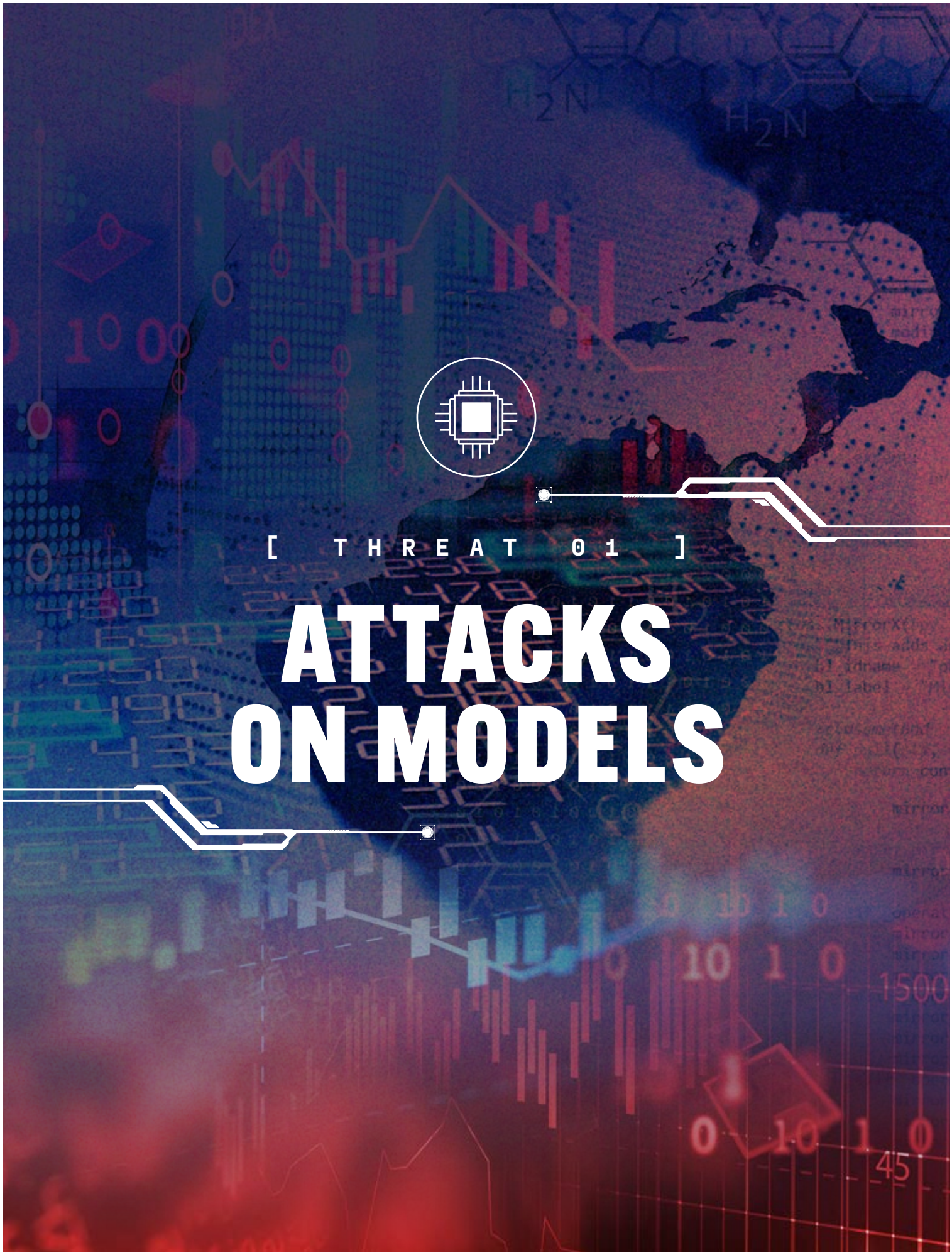
Although there is some overlap between some threats, we view these four threats as differentiated based on their methods and objectives. For instance, we conceptualize *deepfake attacks* as those that involve using advanced technology to alter or fabricate video, audio recordings, images, or text to create a false impression or challenge the authenticity of genuine media. Attackers seek to disseminate this misleading media through social media platforms to influence or manipulate public opinion. In contrast, *memetic engineering* involves the strategic creation or manipulation of ideas, concepts, or beliefs to influence a targeted audience, often relying on psychological triggers or cognitive biases. It is a more targeted attack than a deepfake attack and can be tailored to specific individuals or groups based on their position within social and economic networks. *Attacks on models* are unique in that they target infrastructure rather than individuals or institutions. Their primary aim is to manipulate market outcomes by distorting the AI or ML models that traders and trading algorithms rely on. Finally, *bond dumping* is unique because selling bonds is a legal financial transaction that could be weaponized by an adversary.

In the remainder of this report, we discuss each of the four threats. Using economic theory and historical evidence, we estimate potential costs if each attack were to occur. Finally, we characterize the likelihood of each threat scenario. We base the analysis in each section on the existing literature, as well as the opinions of subject-matter experts. In areas in which little relevant literature exists, we provide more detail on why subject-matter experts believed the threat was relevant and potentially costly and highlight the need for further research.

TABLE 1

Threat Objectives, Targets, and Methods

Threat	Objective	Primary Target	Methods
Attacks on models	Manipulate financial AI and ML models to cause suboptimal trading decisions	Trading models and data sources	Technical exploits, such as data poisoning and adversarial attacks
Bond dumping	Weaken the U.S. economy by selling large amounts of treasury bonds	U.S. bonds market	Sale of a large volume of U.S. treasury bonds
Deepfakes	Use of fake or manipulated media to discredit, extort, or cause panic in financial markets	Consumers, investors, companies, policymakers	Spreading falsified video, audio, text, or images to mass audiences
Memetic engineering	Spread propaganda, memes, and disinformation to undermine U.S. economic stability	Targeted set of consumers, investors, or policymakers	Spreading ideas to targeted audience to change attitudes, beliefs, and behavior


[THREAT 01]
ATTACKS ON MODELS

NEARLY 80 PERCENT OF TRADING VOLUME IN THE UNITED STATES IS EXECUTED BY AN ALGORITHM.[9] Algorithmic trading has opened liquidity access and provision in equities markets to a broader range of participants across multiple trading platforms.[10] AI and its subfield of ML play a prominent role in financial trading because they allow algorithms to quickly process information and make decisions on timescales much faster than humans. Specific models, such as neural networks, are increasingly employed by traders and firms to predict market trends and have been found to perform better than traditional linear models in predicting asset prices and identifying real-time trends and patterns in market data.[11] Neural networks and deep learning models are particularly useful in capturing complex nonlinear relationships and for sentiment analysis in text data, which are critical for strategies like high-frequency trading.[12]

Studies show that algorithmic trading systems have enhanced liquidity and market quality, though they have also created a more complex and integrated market.[13] Higher integration can increase systemic risk, which can make the market more vulnerable to algorithmic failures. For example, the U.S. Securities and Exchange Commission (SEC) described how technological errors in algorithmic trading strategies and automated execution programs (which execute a sale or purchase if market conditions meet a specific set of criteria) in one corner of the market can quickly erode overall market liquidity, particularly in periods of high market volatility.[14]

Adversarial attacks and data poisoning are among the potential reasons for algorithmic failures, both arising from the use of AI and ML in financial trading models. Adversarial attacks are deliberate attempts to manipulate or deceive a neural network by introducing subtle perturbations or noise into its input data.[15] These perturbations can cause the model to misclassify or inaccurately

predict an outcome. In a report on adversarial attacks, OpenAI, the producer of the popular ChatGPT AI tool, notes that defending against adversarial attacks is challenging because there are many (potentially infinitely many) ways that an adversary could manipulate an input that is fed into the model and that creating a model that produces quality output for every possible input is challenging.[16]

Data poisoning attacks are designed to influence a model during the training stage by adding elements into the training data. Unlike adversarial attacks, data poising attempts to "teach" the model incorrect patterns and bias predictions made after training is complete.[17] This means that data poisoning attacks require an adversary to have some knowledge about the model's training data.[18] However, some research has also found that a successful data poisoning attack can be carried out by leaving poisoned data on the internet and waiting for it to be scraped and fed into a model.[19]

POTENTIAL COST

Research finds that adversarial attacks on deep learning trading models can result in substantial financial losses. Xie et al. demonstrates how text-based models that generate public sentiment analysis for traded companies can be fooled by adversarial attacks.[20] By changing just one word in retweets on X (formerly Twitter), attackers can inject subtle false sentiment into the online discourse. The study found that this type of adversarial attack could result in losses in the range of 23 to 32 percent in simulated trading portfolios because it causes the model to make suboptimal trading decisions.

Apart from text data, recent research showed that only a couple of generated, false transaction prices in trading data can alter the response of deep learning models.[21] Using *black-box attack methods*, meaning the attacker does not have access to the original model, Fursov et al. finds that these attacks degrade model accuracy and result in significant financial losses.[22] However, the authors also note that detecting and repelling most of these attacks is relatively straightforward.

Other research has found evidence of attempts to manipulate markets through financial bot activity on X. For instance, there is evidence that financial bots attempt to boost the value of unpopular, low market cap stocks by spreading tweets that mention these stocks alongside popular, high market cap stocks, attempting to lure automated trading algorithms to buy shares of the low-value stock.[23] However, this line of research does not examine whether these financial bots were created by a foreign adversary.

Overall, literature on adversarial attacks suggests that the trading losses that result from feeding a pretrained model false inputs could be large, whether these false inputs are text-based (such as social media posts) or numeric (such as transaction price data). Additionally, prior events—such as the flash crash of 2010—highlight how automated and algorithmic trading can cause market-wide price fluctuations, particularly when volatility in the market is already elevated.[24] Taken together, this suggests that a successful adversarial attack on a firm or industry in one corner of the market could, in theory, cause widespread market disruption. This disruption could be particularly significant if the adversarial attack was timed to occur during a period of market uncertainty (such as the beginning of a pandemic, war, or during a contested election).

The aftermath of the 2010 flash crash led to new volatility controls that might help limit financial losses from such an attack. For instance, in 2012, the national securities exchanges and the Financial Industry Regulatory Authority updated their rules to allow for market-wide circuit breakers in the event of extreme and sudden market downturns. When index prices fall by at least 7 percent from the prior day's closing price, a market-wide circuit breaker is triggered and pauses trading for 15 minutes. For instance, during the onset of the coronavirus disease 2019 (COVID-19) pandemic, the market-wide circuit breaker was triggered four times in ten days.[25]

Assuming that an adversarial attack results in rapid losses substantial enough to trigger a circuit breaker, the 7-percent decline in market value would amount to approximately $2.7 trillion in initial losses.[26] There are additional circuit breakers if index prices continue to fall after the initial

7% DECLINE IN MARKET VALUE ≈ $2.7 TRILLION IN INITIAL LOSSES

15-minute break. Additional protections were also adopted following the 2010 flash crash, including the *limit up–limit down plan*, which functions like a circuit breaker for a single stock, and the short selling–circuit breaker, which prevents short selling from driving down a plummeting stock further. However, some studies caution that markets with circuit breakers can experience increased price volatility compared to those without them.[27]

While there is relatively little research on the potential implications of data poisoning for financial markets, the idea of poisoning historical pricing data was raised in our discussion with subject-matter experts. Some experts suggested that data feeds providing traders and trading algorithms with up-to-date price information could be manipulated to deliver false information to predictive models. However, the consensus in our discussions was that existing redundancy in these data networks would likely render such an attack ineffective at creating long-term disruptions to the U.S. financial system.

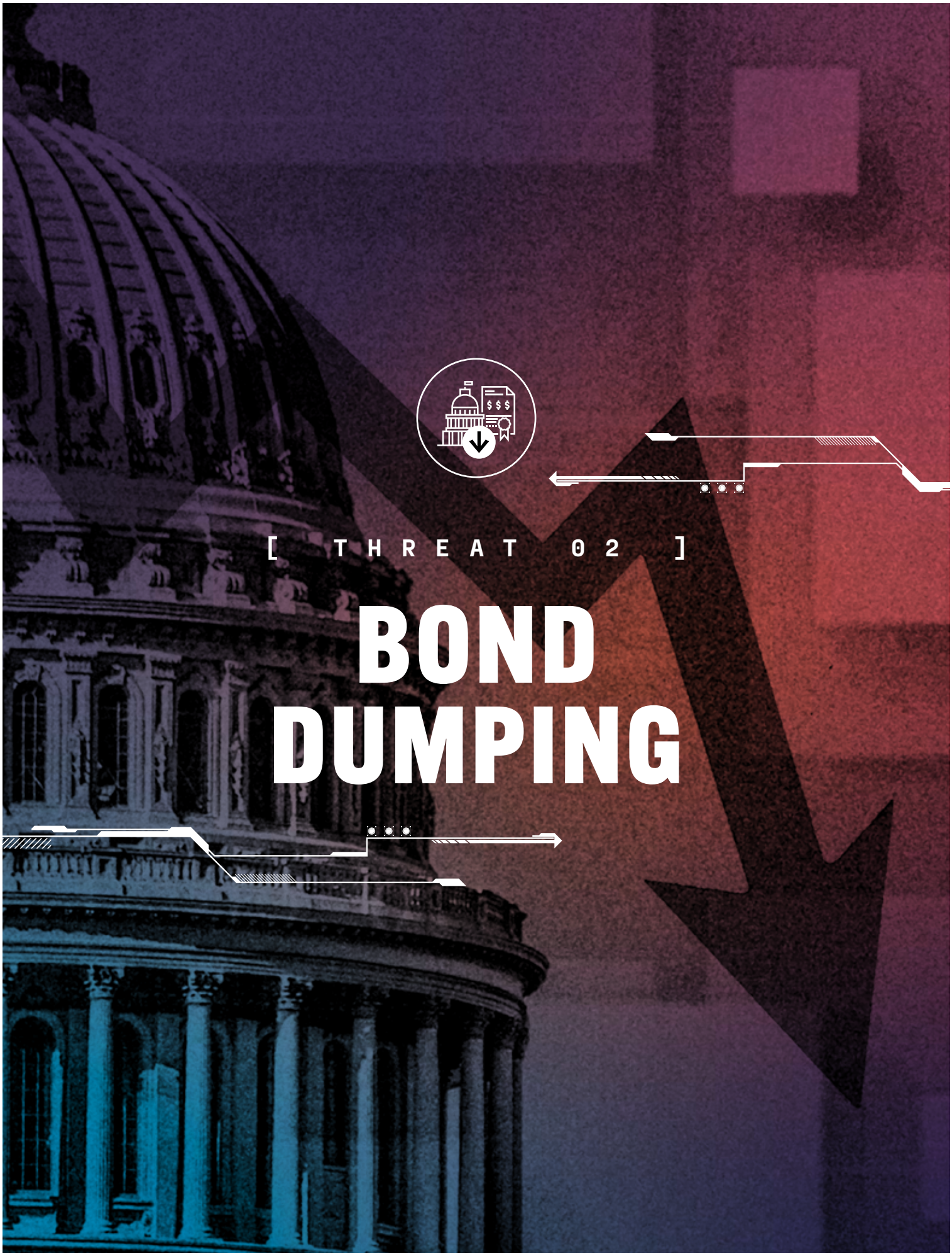
A particularly concerning aspect of a data poisoning attack is the slow speed at which the market might respond. If AI models are trained on faulty data and then used in automated trading algorithms, the model might make inaccurate predictions about which investments are profitable. The losses from these inaccurate predictions might be small and not reach the point at which a market circuit breaker is triggered. However, the cumulative losses over time could still be significant. More research is required in this area to draw firmer conclusions.

FACTORS THAT AFFECT LIKELIHOOD

Several factors influence the likelihood of an attack on financial models. For instance, the development of advanced AI models is concentrated among several leading firms, all of which operate outside the financial sector.[28] This market concentration could give rise to financial sector dependencies on a small number of third-party model providers, creating a new source of systemic risk. For instance, if an adversary were able to successfully poison the training data of a model used by a large segment of the financial sector, the consequences could be larger than if the market for models was more diversified. The SEC chairman has noted the risk posed to financial stability from many institutions relying on the same model or data aggregator.[29]

A factor that might limit the likelihood of an attack is the difficulty of scaling attacks in the real world versus in limited laboratory settings. Laboratory demonstrations offer the strongest evidence for adversarial attacks' potential, but their effectiveness in real-world markets remains largely unproven. Carrying out a successful adversarial attack using text-based inputs would likely require precise timing of the deployment of the artificial messages on a public platform, and the artificial sentiment must not be crowded out by other messages on the platform. Data poisoning might be easier to carry out because an attacker can simply put false data on the internet and wait for it to be used in model training. Although the literature has yet to show what caused losses in the financial sector, the overall effectiveness of this strategy remains unclear.

If AI models are trained on faulty data and then used in automated trading algorithms, the model might make inaccurate predictions about which investments are profitable. The losses from these inaccurate predictions might be small and not reach the point at which a market circuit breaker is triggered. **However, the cumulative losses over time could still be significant.**


[THREAT 02]
BOND
DUMPING

A RECURRING QUESTION IN SOME POLICY DISCUSSIONS IS WHETHER FOREIGN STATES WOULD USE MARKET POWER TO HARM THE U.S. ECONOMY OR U.S. ECONOMIC HEGEMONY—IN PARTICULAR, BY DUMPING U.S. TREASURY BONDS. The possibility was illustrated vividly during the 2008 financial crisis, when Russia urged China to cooperate in dumping U.S. government agency (GSE) debt to further inflame the distressed market.[30] Since then, talk of weaponizing U.S. debt recurred in 2019 in response to China downsizing its U.S. Treasury holdings,[31] and yet again in 2022 and 2023 as China continued to reduce its holdings of U.S. Treasuries.[32]

Bond dumping is different from another concern raised by some commentators, namely, the de-dollarization of markets or payment systems.[33] Unlike de-dollarization, bond dumping would hypothetically be an acute, surprise event for which markets and governments could not plan. The hypothetical story is that a massive, one-time sell-off causes bond prices to plummet, interest rates to rise, and widespread havoc to shake markets. Commentators have presumed that the threat comes solely from China, which holds more U.S. Treasuries than any foreign country except Japan.[34] With optimal strategic timing, China could theoretically raise U.S. government borrowing costs when it needs to expand borrowing—for example, immediately after China precipitates a war with Taiwan.

POTENTIAL COST

The quantitative effects of bond dumping can be estimated based on macroeconomic studies of how interest rates respond to sales of foreign-owned debt. As of June 2023, China owned $835 billion in U.S. Treasuries; for each $100 billion that it sold off, interest rates would rise by 0.26 to 0.71 percentage points.[35] That increase would taper off over the course of the next 12 months. Both empirical studies and historical precedent suggest

that markets could absorb such a shock.[36] This resilience can largely be attributed to the market's size and liquidity, as well as to the promise of Federal Reserve intervention.

For historical examples, consider the 2008 scenario noted above: China and Russia sold off a combined $220 billion in GSE securities late that year, including nearly all of Russia's holdings. This increased interest rates by 1.4 percentage points.[37] However, it was not the once-and-for-all dumping scheme that Russia intended, and the U.S. government response effectively limited the fallout. As another comparison, the Federal Reserve's relatively rapid monetary policy tightening has raised five-year Treasury rates by 4 percentage points since 2020.[38] Based on the estimates above, China would need to sell off at least $500 billion in U.S. Treasuries to generate an interest rate shock of roughly the same magnitude.

In both historical cases, the market absorbed the effects because it is deep and highly liquid. More importantly, in the 2008 scenario, the Federal Reserve intervened to purchase large amounts of assets, thereby stabilizing interest rates and limiting the volatility to the very short term.[39] Even prior to the sell-off, then-Chairman Ben Bernanke noted that the Fed would intervene in such a situation, and the Fed has set a strong precedent for repeating its actions in the future.[40] Therefore, although sharp interest rate increases cause market volatility, particularly affecting bond portfolios,[41] the effects are limited and short-term.

FACTORS THAT AFFECT LIKELIHOOD

We conclude that bond dumping would likely cause short-run volatility and potentially severe losses to some bondholders, but it would not destroy the economy. More importantly, it is highly improbable. This assessment concurs with those from other experts who have discounted the possibility of such a scenario since 2008.[42] First, Russia is no longer a factor. By 2018, Russia had sold off much of its holdings, placing it below the U.S. Treasury's threshold for a "major foreign holder"; as of summer 2023, the U.S. Treasury reported that Russian holdings amounted to just $29 million.[43]

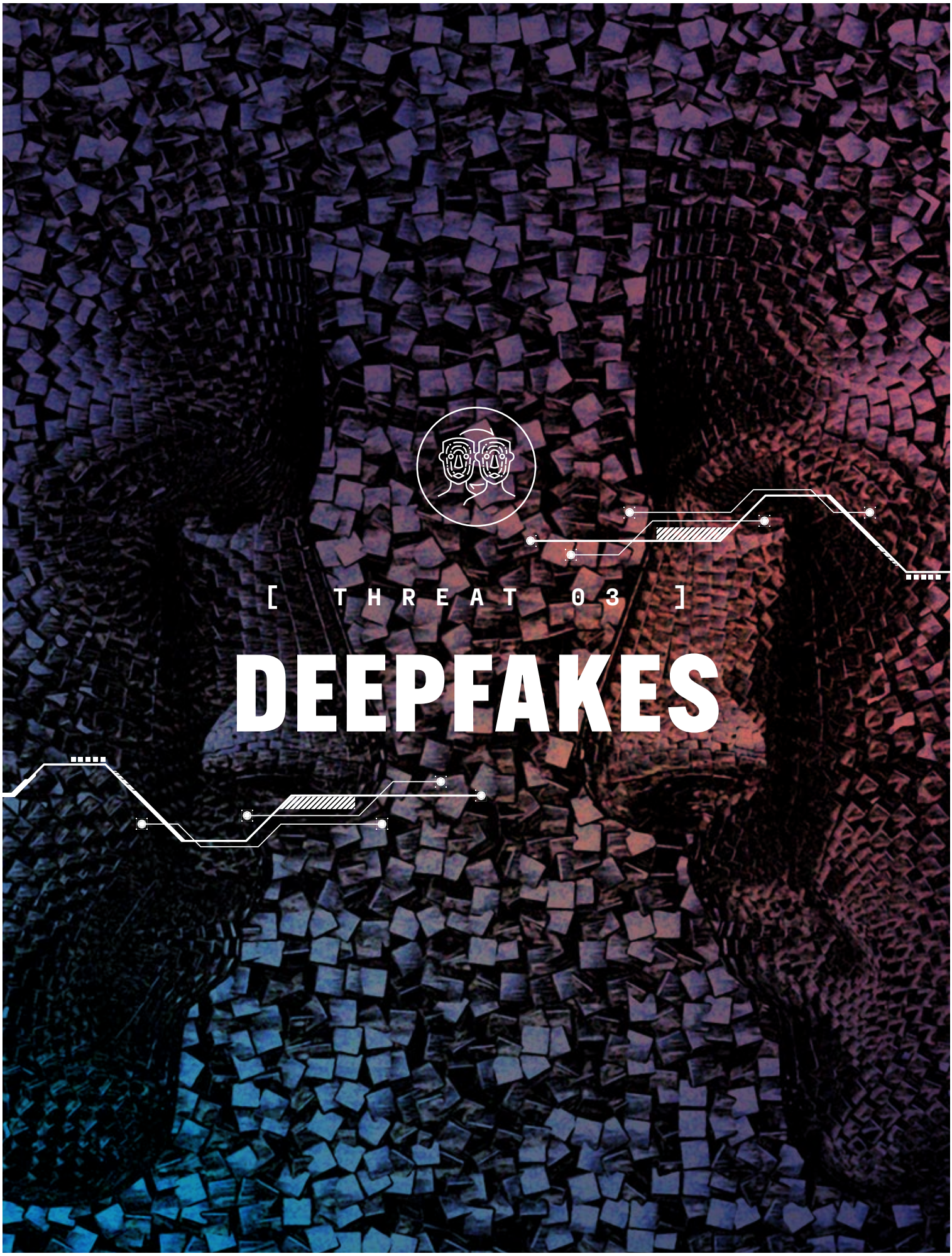
That leaves China as the sole country with the ability—and possible geopolitical incentive—to dump U.S. Treasury bonds in an offensive way. But China has virtually no incentive to do so because it would hurt China more than it hurts the United States or financial markets. China's investment strategy reflects a defensive stance, not an offensive one. China buys U.S. assets and U.S. dollars to make the renminbi more competitive and support export-led growth.[44] At the time of this writing, China's macroeconomy is too weak to gamble on that strategy; in fact, it is so weak that it no longer reports certain fundamental indicators.[45] China's growth is slowing, its youth unemployment is exceedingly high, and additional cracks are appearing in its financial markets.[46]

The threat of a conflict over Taiwan—more than the threat of bond dumping per se—has critical implications for financial stability, but that threat must be countered by geopolitical means, not by financial institutions.

Again, the 2008 GSE sell-off is a useful example. Political scientist Daniel Drezner concluded in 2009 that the sell-off did have some offensive intent as financial statecraft,[47] but it failed to get any meaningful and permanent political concessions from the U.S. government. Since then, Chinese officials have failed to sway U.S. monetary policy, showing that China's market power is insufficient to generate meaningful geopolitical concessions.[48]

Given its macroeconomic conditions, as of September 2023 China has sought to support its currency through a series of changes to bank regulations and U.S. Treasury holdings. It sold U.S. Treasuries in July 2023, continuing this trend from prior months.[49] China also cut its foreign exchange reserve ratio, and state-owned banks have been using U.S. dollars to buy yuan, thereby supporting the strength of its own currency.[50] All these actions are responses to its deteriorating economic conditions, not offensive plays to damage the dollar. Indeed, they have not affected U.S. markets in any substantive way. In July, despite China's net sell-off, total foreign Treasury holdings grew.[51]

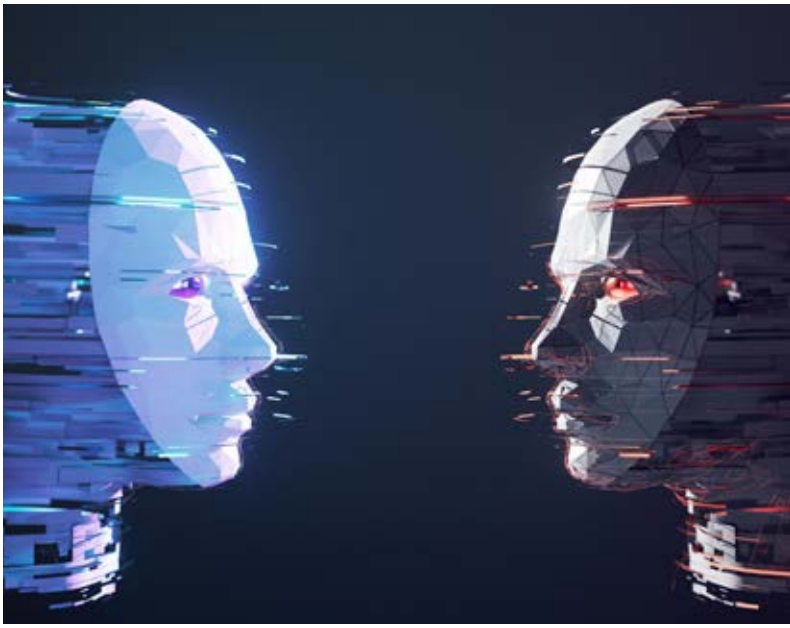
As of September 2023, the geopolitical environment is rapidly evolving, and some experts are reevaluating the likelihood of a U.S.-China conflict over Taiwan.[52] A military conflict or a blockade of Taiwan would have their own economic ramifications, but, in any case, China will be affected by changes in the U.S. dollar's value. The threat of a conflict over Taiwan—more than the threat of bond dumping per se—has critical implications for financial stability, but that threat must be countered by geopolitical means, not by financial institutions.


[THREAT 03]
DEEPFAKES

THE TERM *DEEPFAKE*, A MIX OF THE TERMS *DEEP LEARNING* AND *FAKE MEDIA*, IS COMMONLY USED TO REFER TO DIGITALLY FORGED OR ALTERED VIDEO, IMAGES, DOCUMENTS, OR AUDIO. Deepfakes are typically created using AI tools, which have developed rapidly over the past several years. Not only have deepfakes become easier to create, but their quality has also improved to the point that surveys consistently find people are unable to tell the difference between fake and real media.[53] This technological advancement has triggered concern about the use of deepfakes in spreading disinformation in political contexts, though the threat to financial systems is less studied.[54]

In 2020, the Carnegie Endowment for International Peace convened a roundtable of experts from the financial sectors, technology industry, and regulatory community to discuss the potential future impact of deepfakes on financial markets.[55] The report states that there was disagreement among experts about the feasibility and likely outcome of a deepfake attack on the financial sector; some believed deepfakes were overhyped while others thought they were a critical future challenge facing the financial system. The report ultimately concluded that deepfakes did not pose a current threat to financial stability, but that the risk to individual companies could grow in the future, particularly those facing public relations crises as deepfakes could amplify existing negative sentiment around the company.

Unlike the Carnegie Endowment's panel of experts, the experts in our focus groups and discussions largely held the belief that deepfakes pose a significant risk to financial markets. Several experts offered the perspective that one deepfake could briefly disrupt markets, but an orchestrated deepfake campaign effort might cause deeper and more-lasting harm. Others noted the quality of deepfake detection technology is lagging. This belief seems to be supported by research, though



it is also an area where rapid improvements are occurring. For instance, in a 2020 deepfake detection contest held by Meta, the winning detection model achieved an accuracy of only 65 percent.[56] However, some recent improvements in deepfake detection are occurring, particularly in lip-synching deepfake videos.[57] Intel's deepfake detection technology, FakeCatcher, which uses AI to find indicators of inauthenticity in such biological characteristics as blood flow of the humans depicted, claims to catch 96 percent of video deepfakes.[58]

POTENTIAL COST

In past incidents, deepfakes have caused relatively minor financial damages. One notable example occurred on May 22, 2023, when an image of an explosion outside the Pentagon began circulating on social media. The image first appeared on Facebook but was quickly spread on X (formerly Twitter), including by those posing as the official account of news organizations.[59] Although the

IN 2019, SCAMMERS USED VOICE CLONES TO STEAL:

$667 MILLION
FROM U.S. RESIDENTS

$1.7 BILLION
FROM U.S. BUSINESSES

image was quickly debunked as a fake, it caused the Standard & Poor's (S&P) 500 to drop by 0.3 percentage points in minutes.[60] Smaller scale uses of voice clones, such as real-time deepfake voices, have been used to target individuals (scammers stole $667 million from U.S. residents in 2019 using voice clones), and businesses (U.S. businesses lost more than $1.7 billion because of voice clone fraud in 2019).[61]

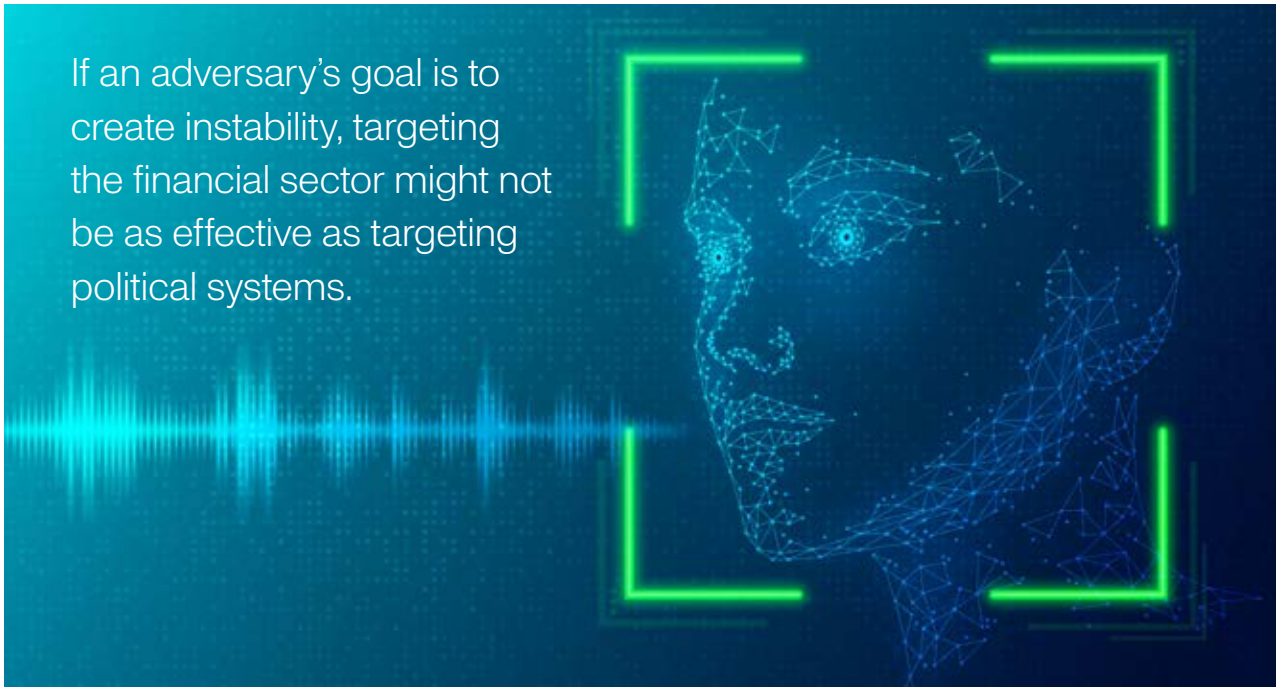
However, both the Carnegie report and our discussions with experts suggest that a coordinated deepfake attack campaign on a company going through a public relations crisis could cause larger-scale financial damage. Paired with social media's capability to quickly erode consumer confidence,[62] the deepfake attack could damage the company's reputation, sales, and share price.

For example, suppose an adversary created a hyper-realistic deepfake video of a highly visible corporate leader of a consumer-facing company making derogatory comments at a private event and then spread the video through verified accounts on X, on Reddit, and through YouTube. Following the initial deepfake video, the adversary then releases forged corporate documents, text messages, audio messages, or additional videos that provide "evidence" of an attempted corporate cover-up of the target's behavior.

Although plausible, it is not immediately clear how much financial damage such a scenario would cause to the targeted company. If the company was already dealing with low trust among the public, it is possible that the attack could cause sales to fall, prompting investors to sell shares. Empirical research on the market response to CEO scandals (including affairs, insider trading, investment fraud, and sexual harassment) suggests that scandals can cause a decline in share prices and increase price volatility in the days following the announcement of the scandal.[63] Other studies have looked at corporate scandals involving the #MeToo movement, finding that the average scandal within the movement led to a short-term decline in stock returns of the affected company by 1.5 percent and a 0.78-percent long-term decline in returns.[64] Although the scandals studied in the literature are real, the findings suggest that a believable deepfake-driven corporate scandal could have moderate financial implications for the affected company.

The implications of this type of attack for the broader market are uncertain. For instance, if the company is highly networked—meaning it plays a meaningful role in national or global supply chains, business transactions, or lending—other stocks could also decline. On the other hand, the degradation to the company's brand could have a positive effect on the stock price of its direct competitors, and the net result on the overall market could be zero.

A coordinated deepfake attack campaign on a company going through a public relations crisis could cause larger-scale financial damage. Paired with social media's capability to quickly erode consumer confidence, the deepfake attack could damage the company's reputation, sales, and share price.

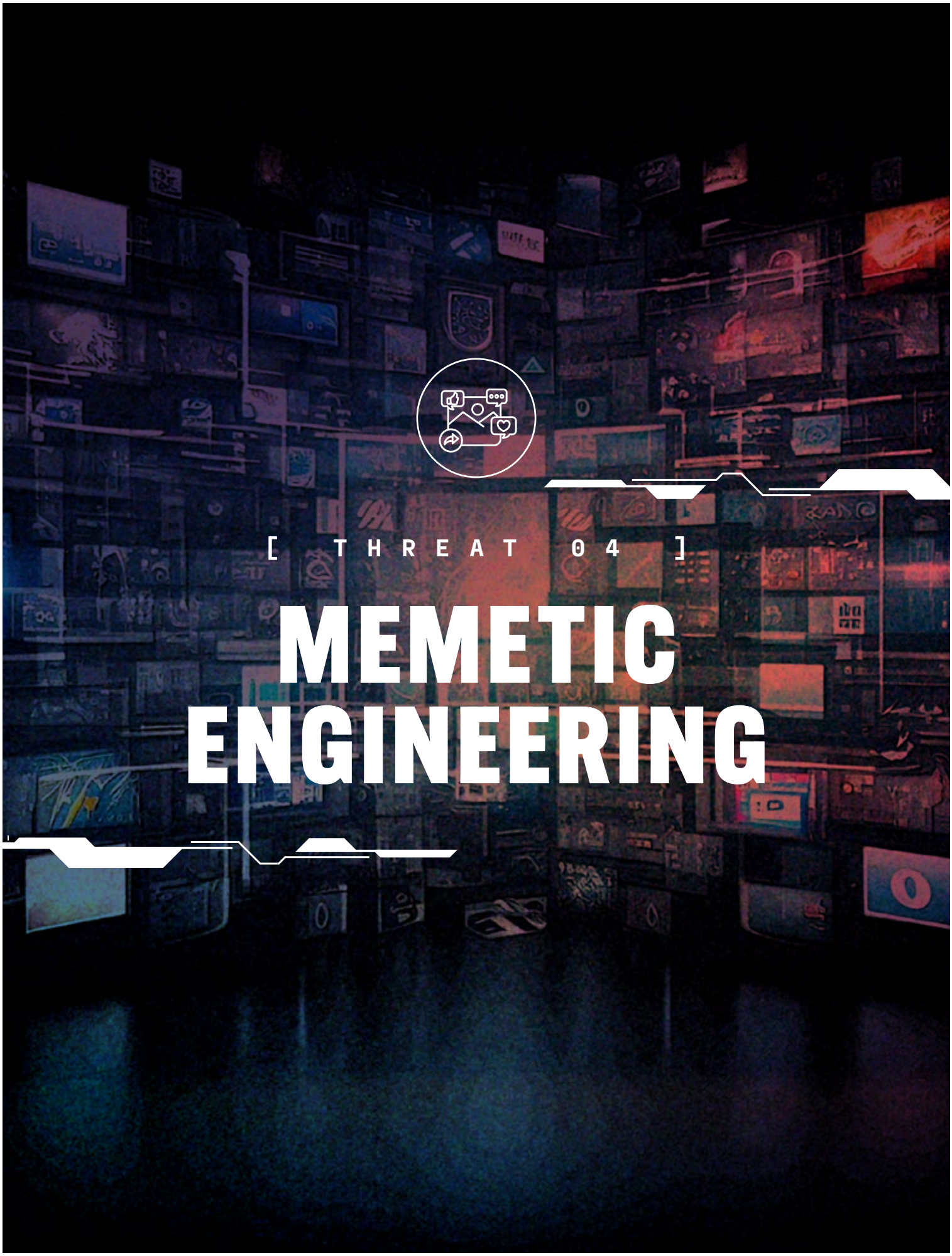


FACTORS THAT AFFECT LIKELIHOOD

Because deepfakes have already affected financial markets to some extent and the AI tools used to create deepfakes are improving rapidly, it is likely that fake images, videos, audio, and text will continue to disrupt markets. However, several factors could amplify the financial impact of deepfakes.

One primary factor is the ability and costs for an adversary to engage in a deepfake campaign involving many deepfakes that potentially span multiple forms of media. The type of campaign discussed above, in which an adversary uses multiple deepfakes to attack a target, could be more costly and difficult than producing a single deepfake. However, the cost of producing believable deepfakes is falling. For instance, voice cloning technology has improved significantly over the past several years and now produces audio that sounds less robotic and might be more difficult to detect.[65] Experts say that deepfake technology has progressed to the point where it can be used in real time without detection.[66] Deepfake videos and images have also become increasingly realistic.[67] As of this writing, the costs of training generative AI models capable of creating realistic deepfakes could deter nonstate actors or nation-state actors with limited budgets from developing their own tools.[68] However, as the cost of developing this technology decreases, or as open-source tools improve, this financial deterrent could become less significant.

A factor that might limit the likelihood of greater deepfake disruptions in financial markets is opportunity costs. Most of the attention paid to the threat of deepfakes has involved risks to political discourse because of the direct correlation between public sentiment and political outcomes.[69] In our discussions with subject-matter experts, some noted that if an adversary's goal is to create instability, targeting the financial sector might not be as effective as targeting political systems. This suggests that the financial system might be more likely to be collateral damage of such an attack than a target. A foreign state deploying a deepfake video of the U.S. President or the Secretary of Defense could rock financial markets, even if the primary goal was to create political chaos. However, while there appear to be more deepfakes directed at public officials than corporate leaders or entities,[70] it is not clear that the costs of attacking both political and financial institutions would prohibit such a deepfake attack.



[THREAT 04]

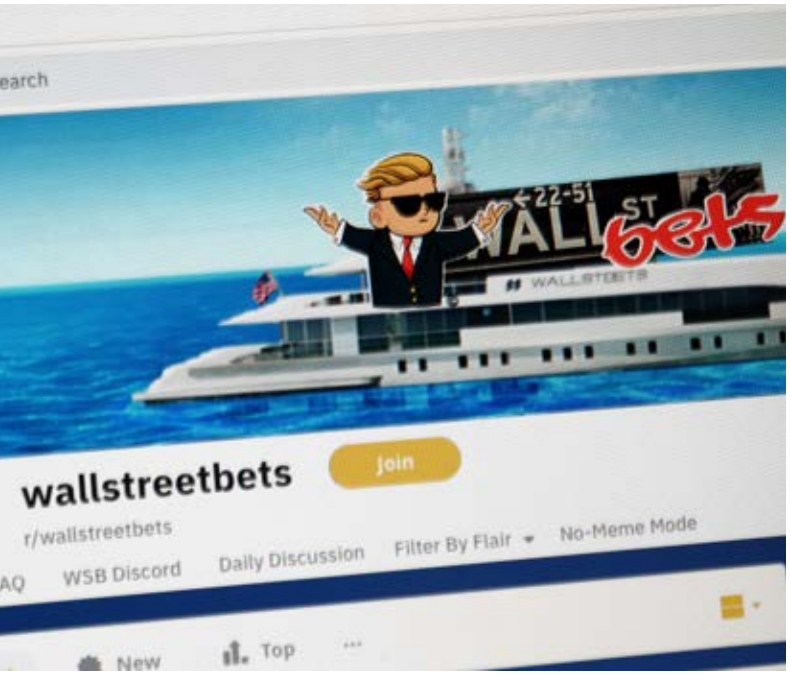
MEMETIC ENGINEERING

MEMETIC ENGINEERING INVOLVES DESIGNING VIRAL IDEAS OR CULTURE (MEMES) TO ACHIEVE A SPECIFIC PSYCHOLOGICAL OR MATERIAL OUTCOME. The term is derivative of genetic engineering, with memes being the cultural equivalent of a biological gene. More specifically, memes are multifaceted units of culture, such as images, videos, phrases, or concepts, that spread rapidly online through imitation and sharing. When weaponized, memes can tap into human tribalism, emotions, cognitive biases, and identity and potentially manipulate behavior or beliefs.[71] Potent memes can shape what issues people focus on, who they see as part of their in-group, and how they direct their energy and anger.

Historically, Russia has been the primary actor in using covert memetic engineering.[72] However, China has begun shifting its focus from social media memetic engineering operations that rely on volume to those that target specific individuals. The 2023 Microsoft Threat Intelligence report notes that Chinese influence operations have begun using generative AI tools to create visual content that has drawn higher levels of engagement in social networks than their prior efforts.[73] The Microsoft report also notes that Chinese operations have expanded across multiple social media platforms, including Reddit, in which many financial discussion boards are hosted.

Although foreign actors have shown increased interest in memetic engineering, there are no reported cases of memetic engineering by foreign adversaries to manipulate financial markets. Additionally, to our knowledge, there have been no analyses of the feasibility of a memetic attack on markets, how an attack might play out, nor the potential economic costs of such an attack. However, in our discussions, subject-matter experts were concerned about the potential for a memetic attack on financial markets because they perceived such an attack to be feasible and potentially impactful.

There are likely two potential use cases of memetic engineering in a financial setting. One is a quick strike attack aimed at creating a rapid frenzy over a specific set of stocks; the other is a longer-term degradation of beliefs, ideologies, or confidence in the market or financial institutions. Although neither of these cases is documented in a financial context, prior memetic engineering efforts outside the financial sector and prior organic meme-driven stock market bubbles have occurred. An example of the former is the Russian company Internet Research Agency's (IRA's) interference in the 2016 U.S. presidential election. As early as 2014, the IRA strategically spread false, polarizing social media content designed for maximum shareability to intentionally manipulate beliefs and actions.[74] The GameStop saga is an example of the latter case. In January 2020, users of the Reddit community r/wallstreetbets sparked a massive rise in the stock price of the video game store GameStop and pushed the "Main Street versus Wall Street" meme around the stock.[75] Although there is no evidence



that foreign agents instigated the GameStop short squeeze on Reddit, there is some evidence that bots pushed GameStop memes on other social media platforms.[76]

An important feature of memetic engineering is the highly targeted nature of the attack. Unlike deepfake attacks, which attempt to spread fake media as widely as possible by broadcasting it through social media platforms, memetic engineering involves narrowcasting a specific idea (a meme) to a specific set of individuals who then spread it to their network. Psychographic data can be compiled from such sources as internet browsing habits, online purchases, and social media interactions and used to craft highly effective messages. Additionally, with such data, ML tools can identify highly influential individuals in social, political, or financial networks. These individuals could then be targeted with personalized and persuasive content.

Some experts we spoke with believed that adversaries can also collect information on market positions and identify the types of stocks that are the most responsive to new information, in which case a memetic engineering attack on the financial sector could be particularly disruptive. However, this is a truly unstudied area in the economics literature, and there is currently no empirical evidence supporting this scenario.

POTENTIAL COST

There is very little evidence—empirical or otherwise—on the costs of memetic engineering attacks. However, there is an emerging line of empirical research on the rapid growth and crash of meme stocks that suggests these stock movements have implications for the broader equities market. Costola, Iacopini, and Santagiustina notes that *meme stocks*—stocks that quickly jump in price and become overvalued because of attention on social media platforms—can exert influence on the broader market by allowing individual retail investors to coordinate and act as a single large trader and that the "mememtentum" that drives meme stock prices can be seen as a form of market manipulation.[77] Others find evidence of spillovers from meme stocks to conventional assets. Yousaf, Pham, and Goodell finds that meme stocks drive shocks to the broader market during periods of extreme upward market movements, but, during meme stock crashes, investors flood to safer assets, such as gold and U.S. Treasuries.[78] Additionally, the authors find that during periods of greater market uncertainty, such as during the onset of the Russia-Ukraine war, the spillovers between meme stocks and conventional assets intensify.[79]

The Federal Reserve Board (Fed) highlighted the risks of meme stocks in the November 2021 Financial Stability Report.[80] The Fed notes that the implication of meme stocks on broader market stability had been limited but also notes that changing regulations, investor demographics, and technology warrant continued monitoring of how meme stocks affect the broader market. The elimination of trading commissions at retail brokerages for stocks and options and the proliferation of mobile trading apps have contributed to the growing share of younger retail investors. Younger investors tend to have higher levels of debt relative to assets, making them vulnerable to large stock price fluctuations. If these younger market participants suffer significant losses from meme stock activities, the adverse effects could spill over into other areas of the financial system, contributing to broader instability.

To our knowledge, there are no studies that provide estimates for the potential cost of

Younger investors tend to have higher levels of debt relative to assets, making them vulnerable to large stock price fluctuations. If these younger market participants suffer significant losses from meme stock activities, **the adverse effects could spill over into other areas of the financial system, contributing to broader instability.**

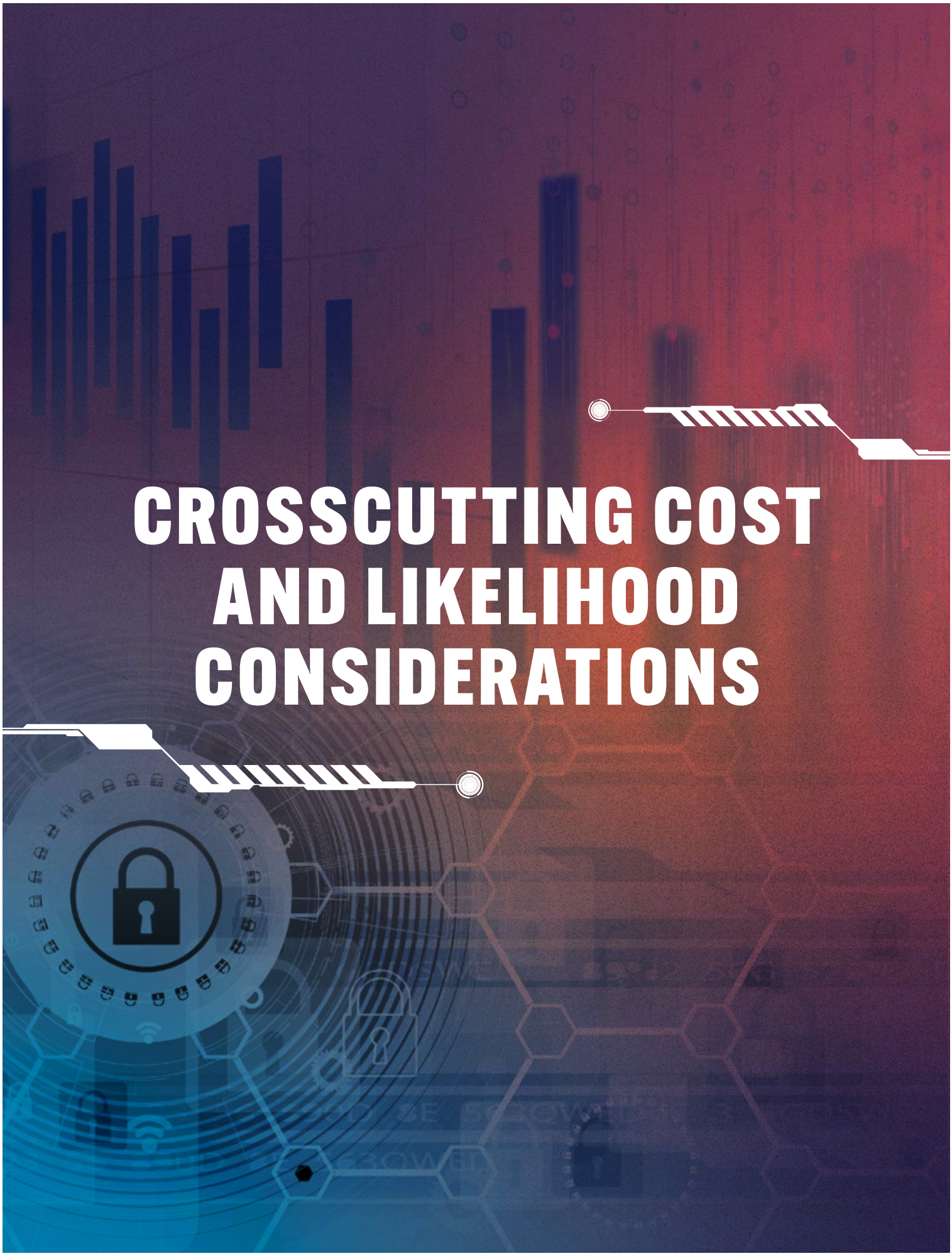
a memetic engineering attack that promotes a longer-term degradation of beliefs and values. Identifying the occurrence of such an attack is challenging because of the latency between when the attack begins and when it manifests in markets. However, the threat of memetic engineering used to degrade trust in markets, institutions, or regulators is a growing concern.[81] Some commentators have suggested that "it is only a matter of time" before foreign actors use memetic attacks to manipulate American markets.[82]

FACTORS THAT AFFECT LIKELIHOOD

Overall, the empirical research on meme stocks suggests that, under specific conditions, a meme stock bubble could have broader economic implications. For instance, research suggests that extreme upward movements of meme stock prices (e.g., price bubble or short squeeze) can cause the price of other assets to grow as well. Depending on the size and nature of these contagion effects, a meme stock bubble burst could cause spillover bubble bursts in other asset classes. If the meme stock's rise coincides with other events that increase market uncertainty, the impact could be magnified.

Another significant factor is the ability to create believable and viral disinformation. Before the advent and adoption of generative AI tools, creating this type of content required human labor, increasing the cost of engaging in such an activity. For instance, the IRA is believed to have hired upward of 400 people.[83] Leveraging generative AI might reduce the number of workers needed to carry out information operations or make workers more effective at producing high-quality content. The continued development of these tools could increase the likelihood of a successful memetic engineering attack. However, some generative AI companies appear to take the risk of misuse seriously.[84]

A second, related factor that could influence the likelihood of a successful attack is the position and protection of consumer data by data-collecting enterprises. Data on purchases, online browsing habits, and social media interactions are essential to building profiles and crafting individualized and highly persuasive content. Collecting this data might be easy in some cases (for instance, if a social media platform is foreign-owned) or may be more difficult (for instance, collecting data on individual credit card purchases). In cases where data collection is more difficult, traditional cyberattacks and hacking may complement memetic engineering actions. However, a single source of data on an individual is likely insufficient to build an accurate profile, meaning that adversaries would likely need to collect data on individuals from a variety of sources. Coordinated efforts across data-collecting entities to prevent the joint use of data by foreign adversaries could slow progress in creating the types of personality profiles needed to engage in highly effective memetic engineering campaigns. Policies to restrict the flow of data to third countries—similar to the European Union's General Data Protection Regulation (GDPR)—could be effective as a coordinating mechanism.[85]



CROSSCUTTING COST AND LIKELIHOOD CONSIDERATIONS

OUR ANALYSIS SUGGESTS THAT THE TOOLS AND METHODS AVAILABLE TO ADVERSARIES TO ATTACK THE U.S. FINANCIAL SYSTEM ARE UNLIKELY TO CAUSE MEANINGFUL MEDIUM- OR LONG-TERM ECONOMIC DAMAGE IN MOST INSTANCES. The most robust lines of defense are the redundancies and safeguards within the financial system, which are explicitly designed to prevent such crises from escalating. Additionally, the global interconnectivity of the U.S. financial system creates a natural deterrence against attack by state actors, though it might not deter nonstate actors, and potential changes in geopolitical relationships could make economic repercussions of an attack less politically costly for adversaries.

Several common themes emerge in the potential costs and likelihood of the threats studied in this report. Each threat has some direct cost associated with it, as well as potential indirect costs to broader markets. Some threats also carry potential intangible costs to social norms or institutions. We also identify several crosscutting likelihood factors. These include technological enablers, situational triggers, and risk management factors that either contribute to or detract from the likelihood of a successful attack.

For each threat, we show these crosscutting factors in Table 2. The direct costs tend to be fairly specific. For instance, a memetic attack might drive up the price of a meme stock, or a deepfake campaign might target a specific business and cause a stock price collapse. The indirect costs arise because of spillovers or contagion effects. In some instances, those spillovers could be positive, such as in the case of a deepfake driving investors to a competitor of the targeted firm. In other cases, the spillovers are likely negative, such as financial contagion effects that could arise from an adversarial attack on financial AI models that spreads through markets, such as the 2010 flash crash. Intangible costs include loss of confidence in specific entities, markets, or financial institutions. These intangible

costs are difficult to quantify because they are highly diffuse and might not directly drive prices in the same way as other attacks that have been studied. Intangible costs are likely most important in the context of memetic engineering but could also emerge in the event of a deepfake attack.

Likelihood factors are shown in the last three columns of Table 2. We group these factors in to three categories: technological enablers, situational triggers, and risk management. Technological enablers are factors that contribute to the likelihood of a successful attack through technological improvement or increased technology integration. For example, a deepfake attack becomes more likely as AI technologies improve, leading deepfakes to become cheaper, more realistic, and harder to detect.

Situational triggers involve preexisting conditions, such as market uncertainty, volatility, or a public relations crisis. Geopolitical tensions are

TABLE 2

Summary of Cost and Likelihood Factors

	COST FACTORS			LIKELIHOOD FACTORS		
	Direct Costs	**Indirect Costs**	**Intangible Costs**	**Technological Enablers**	**Situational Triggers**	**Risk Management**
Attacks on models	• Trade losses because of adversarial attack on financial AI model	• Financial liquidity loss because of contagion effects • Increased market volatility from use of circuit breakers		• Advancing AI • Increased reliance on third-party models	• Preexisting market uncertainty • Increased geopolitical tensions	• Supplemental safety measures to disable AI systems • Market circuit breakers
Bond dumping	• Interest rate increase • Losses on bond portfolios	• Increased stock market volatility • Increased borrowing costs for government and private sectors	• Loss of trust in U.S. Treasury markets		• Increased geopolitical tensions • Increased level of U.S. debt ownership by foreign governments	• Federal Reserve intervention to stabilize markets
Deepfakes	• Stock losses for business targeted by attack	• Potential stock price rise for direct competitors	• Loss of confidence in targeted business	• Advancing AI • Growth of retail investment	• Preexisting public relations issues • Increased geopolitical tensions	• Improvement in deepfake detection technology
Memetic Engineering	• Meme stock bubble from quick-strike memetic attack	• Spillover from meme stock to other assets • Potentially large losses for investors when bubble bursts	• Loss of trust in financial institutions because of slow-burn memetic attack	• Advancing AI • Growth of retail investment • Improved data collection	• Increased geopolitical tensions • Growth of foreign-owned social media platforms	• Increased coordination of data governance

also important situational triggers that can change the motivations of foreign actors by decreasing the political cost that the economic blowback and attack might create. Some subject-matter experts in our focus groups noted that many foreign state actors are unlikely to have the motivation for such an attack, primarily because of foreign entities' stake in the U.S. financial market. An attack aimed at destabilizing the U.S. financial sector could have blowback to the attacking state actor's economy, reducing incentives. However, this lack of incentive is not universal. States outside the U.S. financial system, such as North Korea, or those that are heavily sanctioned, such as Russia, might have the

motivation to harm the U.S. economy and, because of their isolation, not face the economic blowback of the attack. Subject-matter experts also noted that an attack to destabilize the U.S. financial system might be more appealing during war.

Finally, *risk management factors* are mitigation measures that could lower the likelihood or cost of an attack. These involve such factors as supplemental measures to disable financial AI systems, improvements in deepfake detection, circuit breakers to stop market free falls, and coordinated data governance policies. For example, a recent survey conducted by the Artificial Intelligence/Machine Learning Risk & Security (AIRS) Working Group at the Wharton School concludes that numerous financial sector firms are still in the initial stages of AI adoption, and the industry could benefit from increased collaboration in devising risk-reduction strategies.[86] The report emphasizes that governance surrounding the utilization of AI in finance necessitates implementing supplementary safety measures, such as "kill switches" capable of completely disabling the system when required.[87]

CONCLUSION

THE U.S. FINANCIAL SYSTEM IS A FOUNDATIONAL INSTITUTION THAT IS CRITICAL TO THE FUNCTIONING OF THE U.S. ECONOMY, AND PROVIDES LIQUIDITY, INVESTMENT OPPORTUNITIES, AND RISK MANAGEMENT SERVICES TO THE GLOBAL MARKET. However, its position might also make it an attractive target for a foreign adversary. Our assessment of specific emerging threats is that, while the potential for widespread damage exists, most of the threats studied would be more likely to cause more-limited economic losses.

Although concerns about a potential "financial 9/11"—a sudden, catastrophic event with severe consequences—are understandable, our analysis suggests that it is relatively unlikely. Instead, the nature of emerging threats to the U.S. financial system might more closely resemble that of a "financial climate change." This implies a series of gradual, interconnected, and evolving risks rather than an isolated, high-impact incident.

For example, coordinated deepfake campaigns attacking different companies that play out over several years could erode trust in corporate leaders and financial institutions more broadly. Enabled by AI and ML, advanced memetic engineering attacks could progressively undermine trust in financial markets and institutions, causing a steady, incremental impact on market stability rather than a sudden breakdown. Low-profile data poisoning of financial AI models during the training stage could slowly produce suboptimal economic predictions, which avoids triggering market circuit breakers. Geopolitical tensions can create situational triggers that, over time, increase uncertainty and vulnerabilities in the financial system, which leads to a cumulative effect on market performance and overall economic health. While these are speculative risks, their more-gradual nature could also make them more difficult to manage. They may not cause a sudden breakdown, but they could cause a slow decline.

Proactive risk management solutions could prevent losses. Across most threats, advancing AI is likely to play a key role in determining whether an adversary can carry out a successful attack. Thus, policies that encourage the responsible development and use of AI technologies can act as important safeguards to financial stability. The wide variety of risks posed by AI might mean that policies that protect other societal institutions would also provide protection to the financial system. The Biden administration's executive order on safe, secure, and trustworthy artificial intelligence, while not aimed at financial security specifically, outlines new AI safety measures that could protect the financial system from attacks. For instance, the executive order states that extremely large models are required to undergo red teaming exercises and that the results must be submitted to a government regulator. The testing provisions focus on several threats, including the ability of the model to deceive and obfuscate.[88] It is unclear how these new regulations will apply to open-source models. Placing

export controls on advanced semiconductors and requiring cloud service providers to report to the U.S. government if foreign customers appear to be training large models could limit growth of an adversary's AI development as well.[89]

Apart from regulatory policy, economic policies that encourage competition in the AI foundation model market could also increase resilience in the financial sector. Reliance on third-party foundation models could create new sources of systemic risk in the financial sector. Encouraging competition in the market could expand the options available to financial institutions looking to incorporate AI into their operations.

Combating the emergent vulnerability of the gradual erosion of facts in the 21st century, also known as *Truth Decay*,[90] could limit financial exposure to deepfakes and memetic engineering. Research on Truth Decay suggests that analyzing disinformation at the state-actor level,[91] encouraging consumers to seek reliable sources,[92] and political figures with moderate views[93] could limit, stall, or mitigate the effects of Truth Decay. Public awareness campaigns have also been suggested as a policy action that could encourage resilience against deepfakes in a financial setting.[94] However, it is also possible that too much attention to the prevalence of deepfakes could degrade trust in real media. Studying Truth Decay in a financial setting would likely provide new insights into improving financial resilience.

Finally, playing out the potential ramifications, reactions, and counter-reactions to the types of attacks discussed in this report in a wargame scenario would help identify which areas of the U.S. financial system are most vulnerable and why the vulnerability exists. These types of economic wargames could be in the purview of a new civilian "Economic Joint Chiefs," as proposed by Pavel and Egel.[95] Bringing together stakeholders in finance, technology, geopolitics, and national security could result in a new understanding of how these threats might evolve over the next decade.

Rapid developments in AI technology, social media's role in propagating ideas and information into markets, and the growing great-power competition suggest that the financial threats faced over the next decade might become more complex. However, by consistently monitoring and adapting to the changing landscape, embracing technological advancements in a responsible manner, and fostering robust economic policies that promote competition and transparency, the United States will be well positioned to mitigate these emerging threats and maintain its financial stability.

ABBREVIATIONS

AI	artificial intelligence
AIRS	Artificial/Machine Learning Risk & Security
BEA	U.S. Bureau of Economic Analysis
COVID-19	coronavirus disease 2019
Fed	Federal Reserve Board
GDP	gross domestic product
GDPR	General Data Protection Regulation
GSE	U.S. government agency
IRA	Internet Research Agency
ML	machine learning
S&P	Standard & Poor's
SEC	U.S. Securities and Exchange Commission
SVB	Silicon Valley Bank

NOTES

[1] See, for example, Healey et al., *The Future of Financial Stability and Cyber Risk*; Kaffenberger and Kopp, *Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment*; Eisenbach, Kovner, and Lee, "Cyber Risk and the U.S. Financial System."

[2] See, for example, Bateman, "Deepfakes and Synthetic Media in the Financial System."

[3] See, for example, U.S. Department of the Treasury, *The Financial Services Sector's Adoption of Cloud Services*.

[4] See, for example, Osipovich, "After the 9/11 Attacks, Wall Street Bolstered Its Defenses"; Scanlon, *Effects of Terrorism on the U.S. Stock Market*; Johnston and Nedelescu, "The Impact of Terrorism on Financial Markets"; Richman, Santos, and Barkoulas, "Short- and Long-term Effects of the 9/11 Event."

[5] See, for example, Chen, Fang, and Liu, "The Effects of Trump's Trade War on US Financial Markets"; Goodman, "Towards a Smarter Economic Statecraft"; Chivvis and Kapstein, *U.S. Strategy and Economic Statecraft: Understanding the Tradeoffs*.

[6] The SVB collapse took place between March 8 and March 10, 2023. The GameStop short squeeze was a market phenomenon that happened in January 2021, when a group of online retail investors from Reddit's r/wallstreetbets forum drove up the price of GameStop, a struggling video game retailer, by buying shares and options. This caused losses for hedge funds that had shorted the stock.

[7] For instance, after the terrorist attacks on September 11, 2001 (known as 9/11), the U.S. stock market closed for four trading days. Since 9/11, the U.S. financial system has built-in resilience, allowing it to remain open or open quickly following other black swan events. For instance, the market remained open during the COVID-19 pandemic and shut down for only two days following Hurricane Sandy. U.S. Securities and Exchange Commission (SEC) regulations require annual tests of exchanges' disaster plans. See Osipovich, "After the 9/11 Attacks, Wall Street Bolstered Its Defenses." Research on the financial cost of terrorist attacks suggests that the market rebounds relatively quickly. Scanlon found that domestic terrorist attacks cause a significant increase in price variability and a decrease in price levels in the hour following the attack, but that price levels recover within the same day, on average (Scanlon, *Effects of Terrorism on the U.S. Stock Market*). Other studies found a similar result (e.g., Johnston and Nedelescu, "The Impact of Terrorism on Financial Markets"; Richman, Santos, and Barkoulas, "Short- and Long-Term Effects of the 9/11 Event").

[8] See, for example, Baldwin, *Economic Statecraft*.

[9] Li, "80% of the Stock Market Is Now on Autopilot."

[10] SEC, *Staff Report on Algorithmic Trading in U.S. Capital Markets*.

[11] Sirignano and Cont, "Universal Features of Price Formation in Financial Markets."

[12] El Hajj and Hammoud, "Unveiling the Influence of Artificial Intelligence and Machine Learning on Financial Markets."

[13] SEC, 2020.

[14] U.S. Commodity Futures Trading Commission and U.S. Securities and Exchange Commission, *Findings Regarding the Market Events of May 6, 2010*.

[15] Ren et al., "Adversarial Attacks and Defenses in Deep Learning."

[16] Goodfellow et al., "Attacking Machine Learning with Adversarial Examples."

[17] Shabsigh and Boukherouaa, "Generative Artificial Intelligence in Finance."

[18] Wang and Chaudhuri, "Data Poisoning Attacks Against Online Learning."

[19] Shafahi et al., "Poison Frogs! Targeted Clean-Label Poisoning Attacks on Neural Networks."

[20] Xie et al., "A Word Is Worth a Thousand Dollars."

[21] Fursov et al., "Adversarial Attacks on Deep Models for Financial Transaction Records."

[22] Fursov et al., "Adversarial Attacks on Deep Models for Financial Transaction Records."

[23] Cresci et al., "$FAKE: Evidence of Spam and Bot Activity in Stock Microblogs on Twitter"; Tardelli et al., "Characterizing Social Bots Spreading Financial Disinformation."

[24] Trading algorithms and automated execution programs have generated *flash crashes*, a rapid decline and recovery of prices, such as the flash crash of May 6, 2010, in which future and security markets fell 5–6 percent in minutes before recovery just as quickly.

[25] Vereckey, "The Dark Side of Stock Market Circuit Breakers."

[26] We assume a $39 trillion market capitalization for the Standard & Poor's (S&P) 500 index, which captures roughly 80 percent of the overall market capitalization (S&P, "S&P 500"). Although the total market capitalization in 2023 is around $46 trillion, we treat the $39 trillion estimation for the S&P 500 index as if it represents the entire impacted market for the purposes of the attack outlined above (Siblis Research, "Total Market Value of the U.S. Stock Market"). This is because 20–35 percent of trades are not executed algorithmically and—because of the fast-acting nature of the attacks presented—most human traders would not be able to execute trades before markets are shut down.

[27] Chen et al., "The Dark Side of Circuit Breakers."

[28] Vipra and Korinek, *Market Concentration Implications of Foundation Models*.

[29] Palma and Jenkins, "Gary Gensler Urges Regulators to Tame AI Risks to Financial Stability."

[30] Paulson, *On the Brink*.

[31] Rennison and Smith, "Trade War Sparks Fears of China Weaponizing US Treasuries." For related commentary, see LaBrecque, "Are U.S. Treasuries an Assassin's Mace or China's Trump Card?"; Lee, "Ray Dalio Says He Wouldn't Rule Out China Weaponizing Its Massive US Treasury Holdings."

[32] Ma and Woods, "China's Slide of the US Debt Pie"; Sun, "China Cuts US Treasury Holdings to 14-Year Low amid Persisting Security Concerns, Geopolitical Tensions."

[33] Commentators point to several specific events as evidence of the de-dollarization threat: the diversification of central bank reserve holdings, a proposed currency to settle payments among so-called BRICS countries (Brazil, Russia, India, China, South Africa, Egypt, Ethiopia, Iran, and the United Arab Emirates), China's launch of a central bank digital currency (the digital renminbi [e-CNY]), and China's implementation of a new crossborder payments system. See Arslanalp, Eichengreen, and Simpson-Bell, "Dollar Dominance and the Rise of Nontraditional Reserve Currencies."

[34] U.S. Department of the Treasury, *The Financial Services Sector's Adoption of Cloud Services*.

[35] Prior studies estimated the *elasticity of treasury rates*–that is, the percentage change in five-year interest rates to a 1-percent change in foreign ownership. To make elasticities more interpretable, macroeconomists rescale the estimates in dollar terms. Using recent elasticity estimates along with total outstanding treasury securities and U.S. gross domestic product (GDP) as of June 2023, a $100 billion sell-off would increase five-year treasury rates by 26 to 71 basis points; that would taper to 18 to 32 basis points within a year as the market absorbs the shock (a *basis point* is one one-hundredth of a percentage point). See U.S. Bureau of Economic Analysis (BEA), "Gross Domestic Product, Second Quarter 2023 (Advance Estimate)"; Johnson, "Information Disorder Machines"; U.S. Department of the Treasury, *The Financial Services Sector's Adoption of Cloud Services*.

The 71 basis-point figure is calculated based on Ahmed and Rebucci, who estimated a short-run elasticity of 21.8; this amounted to an immediate change in interest rates of 112 basis points based on the total marketable U.S. debt as of 2017 (Ahmed and Rebucci, *Dollar Reserves and U.S. Yields*). Their approach most closely modeled the scenario discussed here: a sudden change in foreign official holdings, controlling for the fact that the Federal Reserve will likely respond. Their estimates were higher than that of others (see Table 1 of their paper), so our own calculations based on their estimates are unlikely to be conservative. The other statistics cited are based on Beltran et al., who calculated an immediate effect of 50 basis points and a 12-month effect of 39 to 62 basis points based on GDP as of June 2007 (Beltran et al., "Foreign Holdings of U.S. Treasuries and U.S. Treasury Yields"). To rescale the estimates, we used data as of June 2023: China's foreign official holdings were $835.4 billion, equivalent to 3.3 percent of all Treasury debt and 3.1 percent of U.S. GDP at the time (U.S. Department of the Treasury, "Table 5: Major Foreign Holders of Treasury Securities"). For a similar calibration exercise and additional details on how and why the effects would be limited by Fed intervention, see Setser, "What Would Happen If China Started Selling Off Its Treasury Portfolio?" In general, estimates vary depending on the method, data, and time horizon used, as well as on whether the researchers control for foreign interest rates or Federal Reserve response.

[36] BEA, "Gross Domestic Product, Second Quarter 2023 (Advance Estimate)"; Johnson, "Information Disorder Machines"; U.S. Department of the Treasury, *The Financial Services Sector's Adoption of Cloud Services.*

[37] Steil and Walker, "The Dangers of Debt."

[38] This change was from a low of 0.19 percent in August 2020 to a high of 4.46 percent by August 2023. See U.S. Board of Governors of the Federal Reserve System, "Market Yield on U.S. Treasury Securities at 5-Year Constant Maturity."

[39] In particular, the government put the GSEs under conservatorship, and the Federal Reserve bought a large amount of GSE debt to stabilize interest rates, as described by Drezner, "Bad Debts."

[40] Morrison and Lebonte, *China's Holdings of U.S. Securities*.

[41] When interest rates rise, bond portfolios can experience high redemption rates and reallocations toward other assets. See Adrian and Oura, "Tracking Global Financial Stability Risks from Higher Interest Rates."

[42] For examples, see Morrison and Lebonte, *China's Holdings of U.S. Securities*; Ikenson, "China's U.S. Debt Portfolio Will Not be Weaponized for the Trade War"; Pettis, "China Cannot Weaponize Its U.S. Treasury Bonds."

[43] U.S. Department of the Treasury, "Table 5: Major Foreign Holders of Treasury Securities." Regarding the 2018 sell-off, see Steil and Della Rocca, who assess whether some of Russia's holdings were diverted to Belgium or the Cayman Islands (Steil and Della Rocca, "Did Russia Really Dump Its U.S. Debt?").

[44] For an explanation and a methodical analysis of why China has no incentive to de-dollarize its reserves, see Pettis, "China Cannot Weaponize Its U.S. Treasury Bonds."

[45] Fu, "China Suspends Report on Youth Unemployment, Which Was at a Record High." As of the last official report, youth unemployment was at 21.3 percent.

[46] Soo, "China's Economy Misses Growth Forecasts, Raising the Odds of More Support for Its Tepid Recovery"; Moreno, "What to Know About China's Real Estate Crisis."

As of the second quarter of fiscal year 2023, GDP growth was lower than expected, foreign investment has dropped,

and major real estate developers have filed for bankruptcy or otherwise shown mounting losses.

[47] Drezner, "Bad Debts."

[48] Drezner also notes that the GSE sell-off partially succeeded in forcing the GSEs into conservatorship but failed in its more ambitious geopolitical goals. See Drezner, "Bad Debts."

[49] Chavez-Dreyfuss, "Foreign Holdings of US Treasuries Increase in July, China Holdings Plunge – Data."

[50] "China to Cut Banks' FX Reserve Ratio to Rein in Yuan Weakness."

[51] Chavez-Dreyfuss, "Foreign Holdings of US Treasuries Increase in July, China Holdings Plunge – Data."

[52] Gordon, Mullen, and Sacks, *U.S.-Taiwan Relations in a New Era.*

[53] Köbis, Doležalová, and Soraperra, "Fooled Twice"; Somoray and Miller, "Providing Detection Strategies to Improve Human Detection of Deepfakes."

[54] Bateman, "Deepfakes and Synthetic Media in the Financial System."

[55] Bateman, "Deepfakes and Synthetic Media in the Financial System."

[56] Canton Ferrer et al., "Deepfake Detection Challenge Results."

[57] Agarwal et al., "Detecting Deep-Fake Videos from Phoneme-Viseme Mismatches."

[58] Intel Newsroom, "Intel Introduces Real-Time Deepfake Detector."

[59] Sorkin et al., "An A.I.-Generated Spoof Rattles the Markets."

[60] Marcelo, "FACT FOCUS: Fake Image of Pentagon Explosion Briefly Sends Jitters Through Stock Market"; Bond, "Fake Viral Images of an Explosion at the Pentagon Were Probably Created by AI."

[61] Bateman, "Deepfakes and Synthetic Media in the Financial System."

[62] Though not caused by a deepfake, the 2023 collapse of SVB underscores social media's capability to quickly erode confidence, demonstrating the potential devastation caused by viral information on financial institutions. Rumors regarding SVB's liquidity circulated on social media, prompting more than $4 billion in deposit withdrawals within 48 hours, and ultimately leading to Federal Deposit Insurance Corporation (FDIC) receivership (Welburn, "Financial Panic in the Age of Digital Banking and Social Media"; Cookson et al., *Social Media as a Bank Run Catalyst*). Although the SVB incident does not directly relate to deepfakes, it sheds light on how social media can rapidly accelerate timelines in financial contexts. The largest bank failure since the Great Recession took place between March 8 and March 10, 2023, with social apps (such as X, WhatsApp, and Slack) fueling fears about the bank's liquidity. This led to withdrawals from venture capital firms and other startup funders (Welburn, "Financial Panic in the Age of Digital Banking and Social Media"; Cookson et al., *Social Media as a Bank Run Catalyst*). The crisis of confidence in the bank highlights the rapid dissemination of financial news through social media and underscores the potential impact of deliberately planted false information on individual companies or markets.

[63] Jory et al., "The Market Response to Corporate Scandals Involving CEOs."

[64] Borelli-Kjaer, Schack, and Nielsson, "#MeToo: Sexual Harassment and Company Value."

[65] Vincent, "This AI-Generated Joe Rogan Fake Has to Be Heard to Be Believed."

[66] Healey, "Real-Time Deepfakes Are a Dangerous New Threat."

[67] Naruniec et al., "High-Resolution Neural Face Swapping for Visual Effects."

[68] Marcellino et al., *The Rise of Generative AI and the Coming Era of Social Media Manipulation 3.0*.

[69] Stanton et al., *The Legal, Ethical, and Efficacy Dimensions of Managing Synthetic and Manipulated Media*.

[70] Bateman, "Deepfakes and Synthetic Media in the Financial System."

[71] Johnson, "Information Disorder Machines."

[72] U.S. Department of Homeland Security, *Homeland Threat Assessment*.

[73] Microsoft, "Digital Threats from East Asia Increase in Breadth and Effectiveness."

[74] Chen, "The Agency."

[75] Biancotti and Ciocca, "Financial Markets and Social Media."

[76] Price, "Bots Hyped Up GameStop on Major Social Media Platforms, Analysis Finds"; Anand and Pathak, "The Role of Reddit in the GameStop Short Squeeze."

[77] Costola, Iacopini, and Santagiustina, "On the 'Mementum' of Meme Stocks."

[78] Yousaf, Pham, and Goodell, "The Connectedness Between Meme Tokens, Meme Stocks, and Other Asset Classes."

[79] Yousaf, Pham, and Goodell, "The Connectedness Between Meme Tokens, Meme Stocks, and Other Asset Classes."

[80] Board of Governors of the Federal Reserve System, *Financial Stability Report*.

[81] Biancotti and Ciocca, "Financial Markets and Social Media."

[82] Lipsky and Wechsler, "The GameStop Saga Is a Road Map for the Kremlin and Other Enemies of America."

[83] Chen, "The Agency."

[84] Goldstein et al., *Forecasting Potential Misuses of Language Models for Disinformation Campaigns and How to Reduce Risk*.

[85] There is an emerging body of literature that suggests that the GDPR has stifled some economic activity (Chen, Frey, and Presidente, "Privacy Regulation and Firm Performance"; Johnson, "Economic Research on Privacy Regulation"); thus, extraterritorial data privacy regulations need to be balanced with opportunities for businesses to engage in legitimate data collection activities.

[86] AIRS, *Artificial Intelligence Risk & Governance*.

[87] AIRS, *Artificial Intelligence Risk & Governance*.

[88] "President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence."

[89] Biden, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence"; Reinsch, Schleich, and Denamiel, "Insight into the U.S. Semiconductor Export Controls Update."

[90] Kavanagh and Rich, *Truth Decay*.

[91] Johnson and Marcellino, *Bad Actors in News Reporting*.

[92] Kavanagh, "Truth Decay Is a Threat to Democracy."

[93] Williams and McCulloch, *Truth Decay and National Security*.

[94] Bateman, "Deepfakes and Synthetic Media in the Financial System."

[95] Pavel and Egel, "A Civilian US 'Joint Chiefs' for Economic Competition with China?"

REFERENCES

Adrian, Tobias, and Hiroko Oura, "Tracking Global Financial Stability Risks from Higher Interest Rates," *IMF Blog*, August 8, 2023. As of September 28, 2023: https://www.imf.org/en/Blogs/Articles/2023/08/08/tracking-global-financial-stability-risks-from-higher-interest-rates

Agarwal, Shruti, Hany Farid, Ohad Fried, and Maneesh Agrawala, "Detecting Deep-Fake Videos from Phoneme-Viseme Mismatches," *Proceedings of the 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2020.

Ahmed, Rashad, and Alessandro Rebucci, *Dollar Reserves and U.S. Yields: Identifying the Price Impact of Official Flows*, National Bureau of Economic Research, Working Paper
No. 30476, September 2022.

AIRS—See Artificial Intelligence/Machine Learning Risk & Security Working Group.

Anand, Abhinav, and Jalaj Pathak, "The Role of Reddit in the GameStop Short Squeeze," *Economics Letters*, Vol. 211, February 2022.

Arslanalp, Serkan, Barry Eichengreen, and China Simpson-Bell, "Dollar Dominance and the Rise of Nontraditional Reserve Currencies," *IMF Blog*, June 1, 2022. As of September 28, 2023:
https://www.imf.org/en/Blogs/Articles/2022/06/01/blog-dollar-dominance-and-the-rise-of-nontraditional-reserve-currencies

Artificial Intelligence/Machine Learning Risk & Security Working Group, *Artificial Intelligence Risk & Governance*, The Wharton School, University of Pennsylvania, November 20, 2022.

Baldwin, David A., *Economic Statecraft*, Princeton University Press, 1985.

Bateman, Jon, "Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios," Carnegie Endowment for International Peace, Cyber Policy Initiative Working Paper Series, No. 7, July 2020.

BEA—*See* U.S. Bureau of Economic Analysis.

Beltran, Daniel O., Maxwell Kretchmer, Jaime Marquez, and Charles P. Thomas, "Foreign Holdings of U.S. Treasuries and U.S. Treasury Yields," *Journal of International Money and Finance*, Vol. 32, No. 1, revised February 2013.

Biancotti, Claudia, and Paolo Ciocca, "Financial Markets and Social Media: Lessons From Information Security," Carnegie Endowment for International Peace, Cyber Policy Initiative Working Paper Series No. 10, November 2, 2021.

Biden, Joseph R., Jr., "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," The White House, October 30, 2023.

Board of Governors of the Federal Reserve System, *Financial Stability Report*, November 16, 2021.

Bond, Shannon, "Fake Viral Images of an Explosion at the Pentagon Were Probably Created by AI," NPR, May 22, 2023.

Borelli-Kjaer, Mads, Laurids Moehl Schack, and Ulf Nielsson, "#MeToo: Sexual Harassment and Company Value," *Journal of Corporate Finance*, Vol. 67, April 2021.

Canton Ferrer, Cristian, Brian Dolhansky, Ben Pflaum, Joanna Bitton, Jacqueline Pan, and Jikuo Lu, "Deepfake Detection Challenge Results: An Open Initiative to Advance AI," *Meta* blog, June 12, 2020. As of August 30, 2023:
https://ai.meta.com/blog/deepfake-detection-challenge-results-an-open-initiative-to-advance-ai/

Chavez-Dreyfuss, Gertrude, "Foreign Holdings of US Treasuries Increase in July, China Holdings Plunge – Data," Reuters, September 18, 2023.

Chen, Adrian, "The Agency," *New York Times Magazine*, June 2, 2015.

Chen, Chinchih, Carl Benedikt Frey, and Giorgio Presidente, "Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally," University of Oxford, Working Paper No. 2022-1, January 6, 2022.

Chen, Hui, Anton Petukhov, Jiang Wang, and Hao Xing, "The Dark Side of Circuit Breakers," *Journal of Finance*, March 23, 2023.

Chen, Yong, Jing Fang, Dingming Liu, "The Effects of Trump's Trade War on U.S. Financial Markets," *Journal of International Money and Finance*, Vol. 134, June 2023.

"China to Cut Banks' FX Reserve Ratio to Rein in Yuan Weakness," Reuters, August 31, 2023.

Chivvis, Christopher S., and Ethan Kapstein, *U.S. Strategy and Economic Statecraft: Understanding the Tradeoffs*, Carnegie Endowment for International Peace, April 28, 2022.

Cookson, J. Anthony, Corbin Fox, Javier Gil-Bazo, Juan Felipe Imbet, and Christoph Schiller, *Social Media as a Bank Run Catalyst*, Université Paris-Dauphine, Research Paper No. 4422754, June 23, 2023.

Costola, Michele, Matteo Iacopini, and Carlo R. M. A. Santagiustina, "On the 'Mementum' of Meme Stocks," *Economic Letters*, Vol. 207, October 2021.

Cresci, Stefano, Fabrizio Lillo, Daniele Regoli, Serena Tardelli, and Maurizio Tesconi, "$FAKE: Evidence of Spam and Bot Activity in Stock Microblogs on Twitter," *Proceedings of the Twelfth International AAAI Conference on Web on Social Media*, Vol. 12, No. 1, June 6, 2018.

Drezner, Daniel W., "Bad Debts: Assessing China's Financial Influence in Great Power Politics," *International Security*, Vol. 34, No. 2, 2009.

Eisenbach, Thomas M., Anna Kovner, and Michael Junho Lee, "Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis," *Journal of Financial Economics*, Vol. 145, No. 3, September 2022.

El Hajj, Mohammad, and Jamil Hammoud, "Unveiling the Influence of Artificial Intelligence and Machine Learning on Financial Markets: A Comprehensive Analysis of AI Applications in Trading, Risk Management, and Financial Operations," *Journal of Risk and Financial Management*, Vol. 16, No. 10, 2023.

Fu, Claire, "China Suspends Report on Youth Unemployment, Which Was at a Record High," *New York Times*, August 15, 2023.

Fursov, Ivan, Matvey Morozov, Nina Kaploukhaya, Elizaveta Kovtun, Rodrigo Rivera-Castro, Gleb Gusev, Dmitry Babaev, Ivan Kireev, Alexey Zaytsev, and Evgeny Burnaev, "Adversarial Attacks on Deep Models for Financial Transaction Records," *KDD '21: Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, August 2021.

Goldstein, Josh A., Girish Sastry, Micah Musser, Renée DiResta, Matthew Gentzel, Katerina Sedova, *Forecasting Potential Misuses of Language Models for Disinformation Campaigns and How to Reduce Risk*, Stanford Internet Observatory Cyber Policy Center, January 11, 2023.

Goodfellow, Ian, Nicolas Papernot, Sandy Huang, Yan Duan, Pieter Abbeel, and Jack Clark, "Attacking Machine Learning with Adversarial Examples," OpenAI, February 24, 2017.

Goodman, Matthew P., "Toward a Smarter Economic Statecraft," Center for Strategic and International Studies, October 29, 2020.

Gordon, Susan M., Michael G. Mullen, and David Sacks, *U.S.-Taiwan Relations in a New Era: Responding to a More Assertive China*, Council on Foreign Relations, Independent Task Force Report, No. 1, June 2023.

Healey, Jason, Patricia Mosser, Katheryn Rosen, and Adriana Tache, *The Future of Financial Stability and Cyber Risk*, Brookings Institution, Cybersecurity Project, October 2018.

Healey, Jon, "Realtime Deepfakes Are a Dangerous New Threat. How to Protect Yourself," *Los Angeles Times*, May 11, 2023.

Ikenson, Dan, "China's U.S. Debt Portfolio Will Not Be Weaponized for the Trade War," *Forbes*, May 22, 2019.

Intel Newsroom, "Intel Introduces Real-Time Deepfake Detector," webpage, November 14, 2022. As of November 16, 2023:
https://www.intel.com/content/www/us/en/newsroom/news/intel-introduces-real-time-deepfake-detector.html

Johnson, Christian, and William Marcellino, *Bad Actors in News Reporting: Tracking News Manipulation by State Actors*, RAND Corporation, RR-A112-21, 2021. As of November 16, 2023:
https://www.rand.org/pubs/research_reports/RRA112-21

Johnson, David, "Information Disorder Machines: Weaponizing Narrative and the Future of the United States of America," Threatcasting Workshop Report, Arizona State University, 2019.

Johnson, Garrett, "Economic Research on Privacy Regulation: Lessons from the GDPR and Beyond," National Bureau of Economic Research, Working Paper No. 30705, December 2022.

Johnston, R. Barry, and Oana M. Nedelescu, "The Impact of Terrorism on Financial Markets," *Journal of Financial Crime,* Vol. 13, No. 1, 2006.

Jory, Surendranath R., Thanh N. Ngo, Daphne Wang, and Amrita Saha, "The Market Response to Corporate Scandals Involving CEOs," *Applied Economics*, Vol. 47, No. 17, 2015.

Kaffenberger, Lincoln, and Emanuel Kopp, "Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment," Carnegie Endowment for International Peace, Cyber Policy Initiative Working Paper Series, No. 4, September 30, 2019.

Kavanagh, Jennifer, "Truth Decay Is a Threat to Democracy. Here's What You Can Do to Help Stop It: Q&A," *RAND Blog*, March 29, 2022. As of September 26, 2023:
https://www.rand.org/pubs/commentary/2022/03/truth-decay-is-a-threat-to-democracy-heres-what-you

Kavanagh, Jennifer, and Michael D. Rich, *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life,* RAND Corporation, RR-2314-RC, 2018. As of September 26, 2023:
https://www.rand.org/pubs/research_reports/RR2314

Köbis, Nils C., Barbara Doležalová, and Ivan Soraperra, "Fooled Twice: People Cannot Detect Deepfakes but Think They Can," *iScience*, Vol. 24, No. 11, 2021.

LaBrecque, Leon, "Are U.S. Treasuries an Assassin's Mace or China's Trump Card? Weaponizing Treasuries in a Trade War," *Forbes*, September 4, 2019.

Lee, Yen Nee, "Ray Dalio Says He Wouldn't Rule Out China Weaponizing Its Massive US Treasury Holdings," CNBC, August 16, 2019.

Li, Yun, "80% of the Stock Market Is Now on Autopilot," CNBC, June 29, 2019.

Lipsky, Josh, and William F. Wechsler, "The GameStop Saga Is a Road Map for the Kremlin and Other Enemies of America—Here's Why," MarketWatch, updated February 2, 2021.

Ma, Adrian, Darian Woods, "China's Slide of the US Debt Pie," *The Indicatory* from *Planet Money* podcast, August 23, 2022.

Marcellino, William, Nathan Beauchamp-Mustafaga, Amanda Kerrigan, Lev Navarre Chao, and Jackson Smith, *The Rise of Generative AI and the Coming Era of Social Media Manipulation 3.0: Next-Generation Chinese Astroturfing and Coping with Ubiquitous AI*, RAND Corporation, PE-A2679-1, 2023. As of September 7, 2023: https://www.rand.org/pubs/perspectives/PEA2679-1

Marcelo, Philip, "FACT FOCUS: Fake Image of Pentagon Explosion Briefly Sends Jitters Through Stock Market," Associated Press, May 23, 2023.

Microsoft, "Digital Threats from East Asia Increase in Breadth and Effectiveness," webpage, September 7, 2023. As of September 29, 2023: https://www.microsoft.com/en-us/security/business/security-insider/reports/nation-state-reports/digital-threats-from-east-asia-increase-in-breadth-and-effectiveness/

Moreno, J. Edward, "What to Know About China's Real Estate Crisis," *New York Times*, August 21, 2023.

Morrison, Wayne M., and Marc Lebonte, *China's Holdings of U.S. Securities: Implications for the U.S. Economy*, Congressional Research Service, RL34314, updated August 19, 2013.

Naruniec, Jacek, Leonhard Helminger, Christopher Schroers, and Romann M. Weber, "High-Resolution Neural Face Swapping for Visual Effects," *Eurographics Symposium on Rendering*, Vol. 39, No. 4, 2020.

Osipovich, Alexander, "After the 9/11 Attacks, Wall Street Bolstered Its Defenses," *Wall Street Journal*, September 7, 2021.

Palma, Stefania, and Patrick Jenkins, "Gary Gensler Urges Regulators to Tame AI Risks to Financial Stability," *Financial Times*, October 14, 2023.

Paulson, Henry M., Jr., *On the Brink: Inside the Race to Stop the Collapse of the Global Financial System*, Business Plus, 2010.

Pavel, Barry, and Daniel Egel, "A Civilian US 'Joint Chiefs' for Economic Competition with China?" *The Hill*, April 23, 2023.

Pettis, Michael, "China Cannot Weaponize Its U.S. Treasury Bonds," Carnegie Endowment for International Peace, May 28, 2019.

"President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence," fact sheet, The White House, October 30, 2023.

Price, Michelle, "Bots Hyped Up GameStop on Major Social Media Platforms, Analysis Finds," Reuters, February 26, 2021.

Reinsch, William Alan, Matthew Schleich, and Thibault Denamiel, "Insight into the U.S. Semiconductor Export Controls Update," Center for Strategic and International Studies, October 20, 2023.

Ren, Kui, Tianhang Zheng, Zhan Qin, and Xue Liu, "Adversarial Attacks and Defenses in Deep Learning," *Engineering*, Vol. 6, No. 3, March 2020.

Rennison, Joe, and Colby Smith, "Trade War Sparks Fears of China Weaponizing US Treasuries," *Financial Times*, May 22, 2019.

Richman, Vincent, Michael R. Santos, and John T. Barkoulas, "Short- and Long-Term Effects of the 9/11 Event: The International Evidence," *International Journal of Theoretical and Applied Finance*, Vol. 8, No. 7, 2005.

S&P—*See* Standard & Poor's.

Scanlon, Kyla, *Effects of Terrorism on the U.S. Stock Market: Evidence from High Frequency Data*, thesis, Western Kentucky University, Spring 2019.

SEC—*See* U.S. Securities and Exchange Commission.

Setser, Brad W., "What Would Happen If China Started Selling Off Its Treasury Portfolio?" *Follow the Money F-25* blog, Council on Foreign Relations, June 21, 2018. As of September 29, 2023: https://www.cfr.org/blog/what-would-happen-if-china-started-selling-its-treasury-portfolio

Shabsigh, Ghiath, and El Bachir Boukherouaa, "Generative Artificial Intelligence in Finance: Risk Considerations," *Fintech Notes*, International Monetary Fund, Vol. 2023, No. 6, August 22, 2003.

Shafahi, Ali, W. Ronny Huang, Mahyar Najibi, Octavian Suciu, Christoph Studer, Tudor Dumitras, and Tom Goldstein, "Poison Frogs! Targeted Clean-Label Poisoning Attacks on Neural Networks," paper presented at the 32nd Conference on Neural Information Processing Systems, Montreal, Canada, 2018.

Siblis Research, "Total Market Value of the U.S. Stock Market," webpage, undated. As of September 29, 2023: https://siblisresearch.com/data/us-stock-market-value/

Sirignano, Justin, and Rama Cont, "Universal Features of Price Formation in Financial Markets: Perspectives from Deep Learning, *Quantitative Finance,* Vol. 19, No. 9, 2018.

Somoray, Klaire, and Dan J. Miller, "Providing Detection Strategies to Improve Human Detection of Deepfakes: An Experimental Study," *Computers in Human Behavior*, Vol. 149, December 2023.

Soo, Zen, "China's Economy Misses Growth Forecasts, Raising the Odds of More Support for Its Tepid Recovery," Associated Press, July 16, 2023.

Sorkin, Andrew Ross, Bernhard Warner, Sarah Kessler, Michael J. de la Merced, Lauren Hirsch, and Ephrat Livni, "An A.I.-Generated Spoof Rattles the Markets," *New York Times*, May 23, 2023.

Standard & Poor's, "S&P 500," S&P Dow Jones Indices, webpage, September 28, 2023. As of September 29, 2023: https://www.spglobal.com/spdji/en/indices/equity/sp-500/#overview

Stanton, Charlotte, Thomas E. Kadri, David Danks, Jack Parker, and Megan Metzger, *The Legal, Ethical, and Efficacy Dimensions of Managing Synthetic and Manipulated Media*, Carnegie Endowment for International Peace, November 15, 2019.

Steil, Benn, and Benjamin Della Rocca, "Did Russia Really Dump Its U.S. Debt?" Council on Foreign Relations, August 13, 2018.

Steil, Benn, and Dinah Walker, "The Dangers of Debt: Russia and China's GSE Dumping," Council on Foreign Relations blog, June 15, 2010. As of September 29, 2023: https://www.cfr.org/blog/dangers-debt-russia-and-chinas-gse-dumping

Sun, Luna, "China Cuts US Treasury Holdings to 14-Year Low amid Persisting Security Concerns, Geopolitical Tensions," *South China Morning Post*, August 16, 2023.

Tardelli, Serena, Marco Avvenuti, Maurizio Tesconi, and Stefano Cresci, "Characterizing Social Bots Spreading Financial Disinformation," in Gabriele Meiselwitz, ed., *Social Computing and Social Media: Design, Ethics, User Behavior, and Social Network Analysis*, Springer 2020.

U.S. Board of Governors of the Federal Reserve System, "Market Yield on U.S. Treasury Securities at 5-Year Constant Maturity, Quoted on an Investment Basis (DGS5)," Federal Reserve Bank of St. Louis, September 28, 2023. As of September 28, 2023: https://fred.stlouisfed.org/series/DGS5

U.S. Bureau of Economic Analysis, "Gross Domestic Product, Second Quarter 2023 (Advance Estimate)," webpage, August 4, 2023. As of October 28, 2023: https://www.bea.gov/news/2023/gross-domestic-product-second-quarter-2023-advance-estimate

U.S. Commodity Futures Trading Commission and U.S. Securities and Exchange Commission, *Findings Regarding the Market Events of May 6, 2010*, September 30, 2010.

U.S. Department of Homeland Security, *Homeland Threat Assessment*, October 2020.

U.S. Department of the Treasury, "Table 5: Major Foreign Holders of Treasury Securities," webpage, undated. As of September 28, 2023: https://ticdata.treasury.gov/resource-center/data-chart-center/tic/Documents/slt_table5.html

U.S. Department of the Treasury, *The Financial Services Sector's Adoption of Cloud Services*, February 8, 2023.

U.S. Securities and Exchange Commission, *Staff Report on Algorithmic Trading in U.S. Capital Markets*, August 19, 2020.

Vereckey, Betsy, "The Dark Side of Stock Market Circuit Breakers," MIT Sloan School of Management, February 16, 2023.

Vincent, James, "This AI-Generated Joe Rogan Fake Has to Be Heard to Be Believed," *The Verge*, May 17, 2019.

Vipra, Jai, and Anton Korinek, *Market Concentration Implications of Foundation Models: The Invisible Hand of ChatGPT,* Brookings Institution, September 7, 2023.

Wang, Yizhen, and Kamalika Chaudhuri, "Data Poisoning Attacks Against Online Learning," arXiv, August 27, 2018.

Welburn, Jonathan W., "Financial Panic in the Age of Digital Banking and Social Media," *RAND Blog*, March 14, 2023. As of September 28, 2023: https://www.rand.org/blog/2023/03/financial-panic-in-the-age-of-digital-banking-social.html

Williams, Heather J., and Caitlin McCulloch, *Truth Decay and National Security: Intersections, Insights, and Questions for Future Research*, RAND Corporation, PE-A112-2, 2023. As of November 16, 2023: https://www.rand.org/pubs/perspectives/PEA112-2

Xie, Yong, Dakuo Wang, Pin-Yu Chen, Jinjun Xiong, Sijia Liu, Oluwasanmi Koyejo, "A Word Is Worth a Thousand Dollars: Adversarial Attack on Tweets Fools Stock Prediction," *Proceedings of the 2022 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies*, July 2022.

Yousaf, Imran, Linh Pham, and John W. Goodell, "The Connectedness Between Meme Tokens, Meme Stocks, and Other Asset Classes: Evidence from a Quantile Connectedness Approach," *Journal of International Financial Markets, Institutions and Money*, Vol. 82, No. 3, January 2023.

PHOTO CREDITS

Page VI: Darren415/Getty Images

Page 2: DKosig/Getty Images, Reptile8488/Getty Images

Page 4: monsitj/Adobe Stock, SergeyBitos/Adobe Stock

Page 5: baona/Getty Images

Page 6: hocus-focus/Getty Images

Page 8: Douglas Rissing/Getty Images, SergeyBitos/Adobe Stock

Page 9: larryhw/Adobe Stock

Pages 10–11: darren415/Adobe Stock

Page 12: vrx123/Adobe Stock, SergeyBitos/Adobe Stock

Page 13: DKosig/Getty Images

Page 15: ArtemisDiana/Adobe Stock

Page 16: pixardi/Adobe Stock, SergeyBitos/Adobe Stock

Page 17: Carsten Reisinger/Adobe Stock, oz/Adobe Stock

Page 18: Marcus Krauss - stock.adobe.com

Page 20: monsitj/Adobe Stock, kras99/Adobe Stock, SergeyBitos/Adobe Stock

Page 21: namning/Adobe Stock

Page 23: sankai/Getty Images

Page 24: ImageFlow/Adobe Stock, matejmo/Getty Images, SergeyBitos/Adobe Stock

Page 25: monsitj/Adobe Stock

Page 26: Alex/Adobe Stock

Back cover: Dilok/Adobe Stock, TAW4/Adobe stock

16.9
13.4
16.8
1.9
RR-A2533-1-V2