CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

NOVEMBER 2021

Cyber Policy Initiative Working Paper Series | "Cybersecurity and the Financial System" #10

Financial Markets and Social Media: Lessons From Information Security

Claudia Biancotti and Paolo Ciocca

Financial Markets and Social Media: Lessons From Information Security

Claudia Biancotti and Paolo Ciocca

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

CONTENTS

Cybersecurity and the Financial System

Carnegie's working paper series 'Cybersecurity and the Financial System' is designed to be a platform for thought-provoking studies and in-depth research focusing on this increasingly important nexus. Bridging the gap between the finance policy and cyber policy communities and tracks, contributors to this paper series include government officials, industry representatives, and other relevant experts in addition to work produced by Carnegie scholars. In light of the emerging and nascent nature of this field, these working papers are not expected to offer any silver bullets but to stimulate the debate, inject fresh (occasionally controversial) ideas, and offer interesting data.

If you are interested in this topic, we also invite you to sign up for Carnegie's FinCyber newsletter providing you with a curated regular update on latest developments regarding cybersecurity and the financial system: CarnegieEndowment.org/subscribe/fincyber.

If you would like to learn more about this paper series and Carnegie's work in this area, please contact Arthur Nelson at arthur.nelson@ceip.org.

Papers in this Series:

- "The European Union, Cybersecurity, and the Financial Sector: A Primer," Philipp S. Krüger and Jan-Philipp Brauchle, March 2021
- "Enduring Cyber Threats and Emerging Challenges to the Financial Sector," Adrian Nish, Saher Naumaan, and James Muir, November 2020
- "Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios," Jon Bateman, July 2020
- "Cyber Mapping the Financial System," Jan-Philipp Brauchle, Matthias Göbel, Jens Seiler, and Christoph von Busekist, April 2020
- "Lessons Learned and Evolving Practices of the TIBER Framework for Resilience Testing in the Netherlands," Petra Hielkema and Raymond Kleijmeer, October 2019
- "Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment," Lincoln Kaffenberger and Emanuel Kopp, September 2019
- "Cyber Resilience and Financial Organizations: A Capacity-building Tool Box," Tim Maurer and Kathryn Taylor, July 2019
- "The Cyber Threat Landscape: Confronting Challenges to the Financial System," Adrian Nish and Saher Naumaan, March 2019

Summary

On January 28, 2021, stocks in U.S.-based video game retailer GameStop Corp. reached an all-time high of $483. Two weeks earlier, they had been trading at $20. Two weeks later, they were down again, and a congressional hearing on the matter was underway in Washington.

Wild swings are hardly uncommon in financial markets. This episode, however, had novel characteristics. In a recent report, the U. S. Securities and Exchange Commission states that "GameStop Corp and multiple other stocks experienced a dramatic increase in their share price in January 2021 as bullish sentiments of individual investors filled social media."[1] Retail traders congregating on the Reddit platform were key in both price formation and the emergence of a "Main Street versus Wall Street" narrative around the stock.[2]

The influence of social media on financial markets is here to stay, as younger generations start saving and investing. This carries both opportunities and risks. Information sharing and discussion on internet platforms can improve market transparency and efficiency. On the other hand, social media platforms are known vehicles of disinformation and manipulation of human behavior. They could be weaponized by malicious actors, ranging from state-sponsored groups to crime syndicates, looking to compromise market integrity and financial stability.

For liberal democracies with independent financial watchdogs, a complex policy challenge follows. In order to fight information operations, financial authorities will need to cooperate with intelligence communities and other relevant parts of executive branches. This requires rules that clearly define each party's role and encourage reciprocal trust.

In many jurisdictions, cybersecurity statutes provide a starting point. They are, however, limited in scope, only covering cooperation vis-à-vis traditional cyber attacks. In this paper, we argue that the model must evolve to help prevent or defend against malicious information operations.[3]
We highlight, as a first step, the importance of organizational modules that allow entities with different levels of access to classified information to work together to assess and inform responses to hostile operations.

Retail Trading and Social Media

Nonprofessional trading has been growing for a few years, partly thanks to new low-cost, user-friendly fintech apps. According to market research firm Apptopia, the top seven trading apps that are not connected to legacy investment firms enjoyed 126-percent growth in U.S.-based downloads between 2015 and 2019.[4] In 2020 and 2021, mobility restrictions related to the coronavirus pandemic translated into further interest in financial apps, both in terms of new users and of daily time spent on the apps by each user. One of the most popular platforms, Robinhood, announced in its June 2021 IPO filing that it had 18 million funded accounts.[5]

Overall, in dollar terms, the phenomenon is still in its infancy. Participants may be legion, yet they invest relatively modest amounts.[6] Nevertheless, retail traders can have a substantial impact when they, as a group, target smaller stocks. Social media offer an opportunity for these groups to form and act at low cost and high speed.

The wallstreetbets community on Reddit has emerged as a key forum for individual traders to exchange investment suggestions and coordinate actions. A few influential users taking an optimistic view of GameStop's prospects were instrumental in building interest in the stock and orchestrating the first rally in early 2021. Before the GameStop episode, wallstreetbets had roughly 2 million subscribers. By July 2021, it had surpassed 10 million.[7] Even as several members suffered heavy monetary losses, vivacious discussion and trading continued.[8]

Virtual trading communities have their own understanding of value. Participants certainly care about returns. Yet, as noted by economist Jayanth Varma, some of them maximize goals other than profit.[9] Their trades are an investment and may also be a political, a moral, or even an emotional statement. Collective beliefs, epitomized in catchphrases and memes, are cemented by online interactions. The epic narrative of ordinary people challenging the powerful looms large. Making money is conflated with making a point, as photos of trades are posted with captions like "just joint the fight" (*sic*).[10]

This attitude partly originates in the crypto-asset world, the original twenty-first-century mixture of techno-utopianism, defiance, and run-of-the-mill profit seeking.[11] Indeed, wallstreetbets and crypto forums share a language, several players, and some trading apps.[12] Although to different degrees, both are at the crossroads between internet phenomena and the formal financial system.[13]

Vulnerabilities

Increasing participation in financial markets and transparent discussion of assets in public forums can contribute to economic growth by improving efficiency in the allocation of capital. The popularization of nonmainstream financial analyses and trading strategies is also, *per se*, potentially positive. In market economies, asset prices reflect an average of different points of view. While this mechanism is expected to be reliable, sometimes it does not work perfectly, and divergent outlooks may be eventually proven correct. Asset valuation models improve over time, occasionally in the wake of such episodes.

When it comes to virtual communities there are, however, certain risks related to how ideas emerge and spread on the internet. Social media provide fertile ground for malicious information operations. Hostile actors can leverage features of online platforms to covertly nudge unaware users toward opinions and actions that serve destructive agendas.[14] In the financial sector, most such agendas would involve erosion of trust—in markets, in individual institutions, or in regulators. While there is no evidence that the GameStop saga was driven by external adversaries looking to disrupt the market, some have argued that the next meme stock frenzy might well be.[15]

Social media are vulnerable to information operations for a number of reasons. First, they use recommendation systems based on what users read and watch, and suggest more of the same. For those with mainstream preferences, recommended content converges to big-name media outlets. For those interested in uncommon ideas, algorithms tend to generate "rabbit holes," or exposure to progressively more extreme theories. Strategically placed ads can accelerate the fall down a rabbit hole. Adversaries who are adept at injecting their views into this system can succeed in creating self-reinforcing bubbles of radicalized users.

Second, despite significant effort by major platform operators, the presence of fake accounts on social media remains a difficult problem to solve. Troll factories, which are large groups of individuals paid to write comments online, can be deployed to create the illusion of sizable, active communities. Artificial intelligence can generate realistic profile photos that depict nonexistent individuals, and it is making strides toward the ability to post articulate, credible text. Inauthentic action has been repeatedly discovered in online discussions of sensitive topics such as race, gender, and the pandemic.[16]

Another significant factor, most evident in specialized discussion boards such as wallstreetbets, is the informal hierarchy among users. A few influencers play a major role in orienting group choices. Adversaries that succeed in recruiting influencers can hold sway over large crowds. This is also true in the offline world, but social media act as a formidable amplifier and accelerator.

The financial sector is a very attractive target for malicious actors of all stripes, a well-established fact in cybersecurity. Attacks against financial institutions or infrastructure are frequent. They offer the potential for monetary gain, exfiltration of sensitive information, and even systemic disruption of the economy.[17] Adversaries may see information operations aimed at distorting price signals, undermining confidence in financial institutions, or otherwise creating disorder, as a means of inflicting the same kind of harm with fewer risks of detection and retaliation compared to traditional cyber campaigns.

Information operations that start off by targeting the financial system can eventually spill over to the political arena. Near-term, domain-specific outcomes—say, high market volatility or inspiration of protests against a single regulatory provision—may reinforce social divisions over broader ideological issues such as the ethical merits of capitalism, the trustworthiness of corporations, and the accountability of governments.

A Challenge for Policymakers

In liberal democracies, preservation of the financial system's integrity and stability generally falls within the remit of independent authorities. This is meant to ensure that regulatory and supervisory decisions, while serving purposes defined by the law, are nonpolitical. Watchdogs have a broad range of conventional instruments to mitigate any risks of disruption *ex ante*, which they are adapting to new technologies.[18] They also have the legal means to tackle standard market manipulation and fraud.

In the face of possible information and influence operations, however, financial authorities cannot and should not work alone. Whenever external actors attempt to interfere with a nation's strategic assets and systems, the problem becomes political. An essential part of the data needed to understand an operation's goal and mechanics is likely to be exclusively available to intelligence communities. Most importantly, decisions on response are a task for executive branches since they channel security policy choices.

The challenge for policymakers is to bring independent authorities and government agencies together to fight information operations in the financial system, leveraging the existing capabilities of each party and introducing new ones where necessary. Cooperation frameworks are needed that clearly define roles and responsibilities, and foster mutual trust.

In several jurisdictions, frameworks are already defined in cybersecurity laws, but they only cover threats to IT systems—unauthorized access, data exfiltration, ransomware, and so on. The model must be expanded and adapted to malicious information operations. The nexus between social media and retail trading offers the starkest example of a vulnerability right now, but it is important to note that the financial system as a whole is a potential target.

Financial watchdogs constantly keep an ear on the ground for anomalies within their supervisory perimeter. For example, market authorities all over the world engage on a continuous basis in market surveillance, a wide array of activities ranging from verification of potentially harmful rumors to real-time deployment of data analytics to detect illicit behavior. Staff in financial watchdogs also already know how to watch for and react to websites and social media accounts deliberately misleading the public on a company or an asset.

These are good starting points, yet some re-skilling has to occur. In particular, influence operations do not necessarily build on lies alone—indeed, they are more credible when they incorporate elements of truth. Financial authorities have to learn the basics of how malicious information manipulation works, so that they can be on the lookout for the right clues. There is a need for threat awareness and at least some diffuse capability for intelligence analysis within all regulatory and supervisory agencies.[19]

Any suspicion of an information operation should be reported via structured channels to the intelligence community for further analysis and, where applicable, attribution. In traditional cybersecurity, the toughest part is finding the culprit(s) of an attack, who are often obfuscated by layers of hijacked machines and unaware accomplices. This applies *a fortiori* to information operations. Once conclusions are reached, they must be passed on to the relevant level of government for response decisions.

One important choice to be made is: to which extent should independent authorities stay involved in the process of investigating the operation, after they have alerted the government and provided a first round of data and evaluations? A delicate balance must be struck between protecting confidentiality, leveraging specialist skills, and avoiding frictions across institutions, while staying true to the legal mandate of each party.

Preferred solutions would likely vary across countries, even within like-minded groups such as the G7. It is nonetheless possible to find some common patterns across different systems and draw lines of reflection, at least in terms of principles. From a procedural point of view, it is crucial that this issue is settled transparently from the beginning. Factors that need to be considered include, but are not limited, to the following:

(i) government agencies, independent authorities, and other potential participants in the process—for example, private sector entities or academia—have different levels of access to classified and otherwise sensitive information;
(ii) information must be passed along to participants on a need-to-know basis;
(iii) the effectiveness and fluidity of information exchanges need to be maximized; and
(iv) process separation must exist between information gathering, analysis, and response.

These constraints require a flexible organizational module, which enables differentiated access to information across participants. In several countries, current practice in homeland security foresees so-called "fusion centers" or "fusion cells," hubs where data and capabilities of heterogeneous actors are jointly leveraged for a given goal.[20] Fusion centers can involve participants outside of intelligence and law enforcement, such as health authorities or private companies.[21] The model could be adapted to include stakeholders from the financial sector. It could also envision appropriate modes of participation for platform operators, since they have access to crucial data on users, and for qualified communities of independent investigators, such as from academia. Depending on the jurisdiction, fusion centers may build on preexisting, cyber-related information sharing arrangements.

Conclusions

Finance-focused virtual communities are growing in size and potential economic and social impact, as demonstrated by the role played by online groups of retail traders in the GameStop case. Such communities are highly exposed to manipulation, and may represent a prime target for state and nonstate actors conducting malicious information operations.

Sophisticated information operations carried out online may be very hard to distinguish from spontaneous behavior. Financial authorities should learn the basic elements of how malicious information operations work, and act as a first line of detection and defense. An appropriate legal framework should be in place so that sector watchdogs can contribute data and specialist knowledge to governmental actors tasked with analysis of and response to information operations. This can be achieved by implementing organizational modules that allow entities with different levels of access to classified information to work together and, in several jurisdictions, by adapting existing legislation on cybersecurity.

About the Authors

Claudia Biancotti is a director at the Bank of Italy.

Paolo Ciocca is commissioner at Consob, the Italian financial market regulator, and a nonresident scholar at the Carnegie Endowment for International Peace.

Acknowledgments

The opinions expressed in this paper are personal and should not be attributed to the Bank of Italy, Consob, or the Carnegie Endowment for International Peace. The authors would like to thank Giuseppe Ferrero, Arthur Nelson, Mario Rasetti, Michele Savini Zangrandi, Giovanni Veronese, and three anonymous reviewers for useful insights and suggestions.

Notes

1 "SEC Staff Releases Report on Equity and Options Market Structure Conditions in Early 2021," U.S. Securities and Exchange Commission, October 18, 2021, https://www.sec.gov/news/press-release/2021-212.

2 Other listed companies, such as AMC Holdings and BlackBerry, were involved in similar dynamics.

3 For a discussion of terminology relating to how information is used to influence target audiences, see Alicia Wanless and James Pamment, "How Do You Define a Problem Like Influence?," *Journal of Information Warfare* 18, no. 3 (2019): 1–14, https://carnegieendowment.org/files/2020-How_do_you_define_a_problem_like_influence.pdf.

4 Adam Blacker, "Robinhood Now Has More Mobile Monthly Active Users Than the Top Legacy Providers Combined," Apptopia, January 6, 2020, https://blog.apptopia.com/robinhood-now-has-more-mobile-monthly-active-users-than-the-top-legacy-providers-combined.

5 "United States Securities and Exchange Commission, Form S-1 Registration Statement, Robinhood Markets, Inc.," U.S Securities and Exchange Commission, July 1, 2021, https://www.sec.gov/Archives/edgar/data/1783879/000162828021013318/robinhoods-1.htm.

6 IHS Markit, a financial data firm, estimates that "individual-driven, pure play retail accounts" commanded roughly 3 percent of total trading volume on U.S. stock markets between January 2020 and January 2021. Volume is computed based on "changes to custodial positions at Charles Schwab, E*Trade, Interactive Brokers, National Financial (Fidelity's retail arm), Robinhood, TD Ameritrade, and Wells Clearing custodians." It does not reflect intraday trading, or individual investment mediated by professional wealth managers. IHS Markit does not specify the reference market(s). According to Reuters, investment bank Morgan Stanley puts the figure at a much higher 10%–15% for the Russell 3000 index. The computation methodology is not publicly available. See "Retail Investor Trends: Revisiting the Impact of Retail Activity," IHS Markit, March 1, 2021, https://ihsmarkit.com/research-analysis/retail-investor-trends-revisiting-the-impact-of-retail-activity.html; Thyagaraju Adinarayan, "Retail Traders Account for 10% of U.S. Stock Trading Volume – Morgan Stanley," Reuters, June 30, 2021, https://www.reuters.com/business/retail-traders-account-10-us-stock-trading-volume-morgan-stanley-2021-06-30/.

7 Not all subscribers are active in discussions, but installing the Reddit app on a smartphone and joining a subforum, or subreddit, implies exposure to content notifications on a somewhat regular basis.

8 For example, Robinhood was still in Google Play's top 100 chart in the spring of 2021.

9 Jayanth Varma, "The Rationality of r/wallstreetbets," Prof. Jayanth R. Varma's Financial Market's Blog, January 31, 2021, https://jrvarma.wordpress.com/2021/01/31/the-rationality-of-r-wallstreetbets/.

10 Novabud, "Just Joint the Fight #GME STAY STRONG," Reddit, March 5, 2021, https://www.reddit.com/r/wallstreetbets/comments/lyfh2x/just_joint_the_fight_gme_stay_strong/.

11 Nick Paumgarten, "The Prophets of Cryptocurrency Survey the Boom and Bust," *New Yorker,* October 15, 2018, https://www.newyorker.com/magazine/2018/10/22/the-prophets-of-cryptocurrency-survey-the-boom-and-bust.

12 GameStop and other so-called meme stocks are traded in regulated markets. Bitcoin is not but, in the quasi-normalized version of today, it is traded by some professional investment firms following strategies that have long been employed for other high-volatility instruments, without any connection to the cryptocurrency's original spirit. The appearance of normalization is reinforced by a few high-visibility brands choosing to accept Bitcoin as a means of payment—it is, however, important to note that Bitcoin is not legal tender, with the sole exception of El Salvador. See Robin Wigglesworth and Eva Szalay, "'Digital Tulip' or New Asset Class? Bitcoin's Bid to Go Mainstream," *Financial Times,* February 12,

2021, https://www.ft.com/content/7ac6c3a6-3fed-4dd9-8a69-939ad6094933.

13 Wallstreetbets also has a measure of contiguity with other controversial corners of the internet. The forum's tagline is "Like 4chan found a bloomberg terminal" (sic), a reference to a now-defunct platform famous for hosting inflammatory content and favoring divisive, politically charged verbal extremes. Similar affinities exist in parts of the crypto world, especially where technical decentralization is translated into an anti-system sentiment.

14 This subject is discussed in a large and growing literature. Summarizing it is beyond the scope of this work. For an introduction to research methods in this field, see Technology and Social Change Research Project Team, "The Media Manipulation Casebook," Harvard University, https://mediamanipulation.org/about-us. For a nontechnical primer, see for example P. W. Singer and Emerson T. Brooking, *Likewar: The Weaponization of Social Media* (Boston: Houghton Mifflin Harcourt, 2018).

15 Some retail traders appear aware of the problem, as shown by Russian spy-themed memes during the March 2021 wallstreetbets craze around U.S. defense contractor Palantir. Also see Josh Lipsky and William F. Wechsler, "The Gamestop Saga Is A Road Map For The Kremlin And Other Enemies Of America — Here's Why," MarketWatch, February 1, 2021, https://www.atlanticcouncil.org/insight-impact/lipsky-and-wechsler-in-marketwatch-the-gamestop-saga-is-a-road-map-for-the-kremlin-and-other-enemies-of-america-heres-why/.

16 On the pandemic and vaccines, see for example European Union External Action Service, "EEAS Special Report Update: Short Assessment of Narratives and Disinformation Around the Covid-19 Pandemic, April 2021, https://euneighbourseast.eu/news-and-stories/publications/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid-19-pandemic-update-december-2020-april-2021/.

17 Also see Tim Maurer and Arthur Nelson, "International Strategy to Better Protect the Financial System Against Cyber Threats," Carnegie Endowment for International Peace, November 18, 2020, https://carnegieendowment.org/2020/11/18/international-strategy-to-better-protect-financial-system-against-cyber-threats-pub-83105.

18 On those, one issue that warrants special attention today is transparency with regard to business models, potential conflicts of interests, and the treatment of customer data. There may also be scope for innovation in disclosure requirements for asset issuers. Perhaps potential investors are entitled to know if a company can count on the support of r/wallstreetbets or Twitter, the way they must be informed of changes in funding or ownership. A reflection is needed on the shifts in risk appetite induced by a sizable influx of small investors.

19 This is urgent in areas where information plays a key role, such as finance, but also applies to other strategic economic branches. Social media are everywhere, influence operations can be anywhere.

20 For example, the U.S. Department of Justice defines a fusion center as a "collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity." "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era," U.S. Department of Justice, August 2006, https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/fusion_center_guidelines_law_enforcement.pdf.

21 "Nontraditional collectors of intelligence, such as public safety entities and private sector organizations, possess important information (e.g., risk assessments and suspicious activity reports) that can be "fused" with law enforcement data to provide meaningful information and intelligence about threats and criminal activity." From "Fusion Center Guidelines," U.S. Department of Justice.

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org