

CYBER COVID ESEJ

How Combination of High-Frequency Trading and Disinformation Could Cause Next Economic Crisis

The world is becoming increasingly more interconnected and thus it is logical to ask what type of cyber-attack has disruptive potential comparable to the recent and still ongoing COVID-19 pandemic.

Since the inception of the pandemic, we can observe relative ease with which [different actors](#) were able to “infect” people with panic and uncertainty using [intentional and non-intentional misinformation and disinformation](#). This is an evidence of significant potential of disinformation campaigns to [rapidly spread globally](#).

It is the combination of rapidly spreading serious disinformation and interconnectedness especially present in the financial sector that has the power to cause wide systemic breakdown such as an economic crisis. This danger is further magnified by the relatively new form of trading, so called [High-frequency Trading \(HFT\)](#).

This essay will focus on how using social media power and hacking media organizations can cause next economic crisis, especially when combined with HFT platforms systemic disruption potential.

Following the 2008 crash new trading system, the HFT has been introduced to rapidly create liquidity in the markets. HTF systems use extremely capable computers to

execute large volume of trades every second. This type of trading is very controversial as it puts smaller players who does not use HFT in unfavourable position, yet nowadays is deeply embedded in the financial sector. For instance, in the US, machine-led trades formed approximately 80% of stock activity in 2018, according to [CNBC report](#), with specifically HFT counting for approximately 50% of stock activity in 2019 according to the [Franklin Templeton](#) investment company report. [The Atlantic report](#) from 2019 approximated the percentage globally to be around 50%.

The core problems lay with the algorithms based on which the trades are being executed. Even though the precise algorithms are not publicly available it is known that they, among other things, [analyse news, social media and use linguistic analysis](#) of the large part of the internet. This means that when some specific key words or combination of words are being repeatedly shared during a short period, HFT will react within fractions of second. When a robust and rapidly spreading disinformation hits the internet, HFT platforms will respond to the situation in an extremely short time, causing other systems or salesmen to follow along therefore magnifying the risk of systemic breakdown.

Imagine a scenario, major international media organization's social media are hijacked by an unknown hacker. He posts an extremely alarming piece of information, which is likely to be shared and read by millions of people in next minutes as such media have large number of followers on their social media.

There actually is an example of such situation. In 2013, [Associated Press News Agency's Twitter account was hacked](#) by an unknown group of hackers who posted information about explosions in the White House. This example had a [short term yet very strong impact on the markets](#). Part of the reason was the HFT, which reacted minutes before the human staff knew about the incident. As stability is of paramount importance in the markets, unreasonable behaviour of the HFT algorithms will without any doubt cause a lot of chaos. For their complexity it also may take tens of minutes or even several hours to analyse and understand seemingly unreasonable behaviour of the HFT algorithm. At that time hundreds of millions of dollars might be already lost.

The media are the second equation of the problem. Even though communication infrastructure is considered to be a part of the Critical Information Infrastructure (CII) in

most countries, social networks and media organizations themselves are usually not considered to be one. This raises serious questions, because as we have just examined, even one hacked post on Twitter or Facebook page of powerful media such as the AP, CNN, Reuters, and others might have a massive impact on economy of different countries, possibly even starting an economic crisis.

The fact that commercial media organizations not usually protected under various cybersecurity laws probably comes from the understanding that media do not provide people with essential needs. This is the case with hospitals, power plants or freshwater facilities that may directly cause people to die or suffer. However, media provide the world with information in real time, which represents especially crucial capability in the time of crises such as the one we have seen with the COVID-19. Moreover, media have an ability to create a trust and stability, but also have a significant disruptive potential if compromised.

To conclude this essay, I would like to highlight several points from previous text and add recommendations to implement to diminish or at least limit examined vulnerabilities in the financial sector.

Firstly, it is crucial to understand that financial system is very much dependent on the HFT system and a significant amount of trades is being executed by machines and algorithms. Increasing complexity of these trades makes the financial system more vulnerable to various threats as it prolongs the ability of the human staff to react and solve the issues that may emerge.

The HFT system got an attention of regulators after events such as the [Flash crash in 2010](#), where algorithms played a prominent role. Different example was the [Knight Capital case in 2012](#), where faulty algorithm cost the company 440 million dollars in 45 minutes.

As the technology is still very new, the regulations are not keeping up. Even though there are provisions on loss-stopping measures, [little regulation on the speed of the trades](#), key aspect of the HFT, were introduced. It is therefore important to limit the HFT's trading speed and possibly further regulate the number of trades to be executed over a certain period.

Secondly, media and social media are part of the financial sector itself as algorithms, which lead around 50% of all stock activity globally, take information from big data analysis of both news sources and social media.

When we acknowledge this fact and interconnectedness of both market and media, it is logical that social media and influential traditional media should become a part of the CII or receive protection. Their ability to cause economic damage, magnify it (especially when counting in the HFT) but also to revive trust of the people and investors, is crucial.

Even in case various smaller crashes might not cause a major economic crisis, combined they have the potential to decrease trust in the financial system as a whole. What is more, aforementioned vulnerabilities are theoretically exploitable by a single well-informed individual who has an extensive knowledge of the HFT automation processes.

Our civilization is increasingly dependent on automation, using various media to trick algorithms to quickly sell-buy based on false information therefore pose a real danger to the financial system. Limiting systemic disruptive potential of the HFT, spread of disinformation, and protecting media are some of the key steps to effective protection of the state economy.