STOCK MARKET CYBERCRIME

DEFINITION, CASES AND PERSPECTIVES

ALEXANDRE NEYRET

AUTORITÉ
DES MARCHÉS FINANCIERS
AMF

Summary

For several years, and the subject has often been referred to in the press, cybercrime has been invading our world. The financial sector and more especially the stock market sector are no exception. Every year, new stock market “cyberattacks” (insider trading by hacking confidential information, the dissemination of false financial information influencing the share price of a listed company by creating “fake” websites or fake rumours on social media, the manipulation of financial instrument prices by hacking trading terminals, etc.) continue to appear. It was therefore crucial to try to provide an overview of stock market cybercrime in order to better understand the modi operandi and the problems of potential stock market breaches with a “cyber” component, which the Autorité des Marchés Financiers (hereinafter referred to as the “AMF”) may have to deal with.

After defining stock market cybercrime and obtaining an estimate of the cost of cybercrime (in general) and of the impact of a cyberattack on a listed company’s share price, we analysed the various cases available publicly, sometimes trying to anticipate the future of cyber insider trading, cyber price manipulation and cyber dissemination of false information.

Finally, a summarised mapping accompanied by an analysis of the factors contributing to stock market cybercrime demonstrates its future importance and its impact on the entire stock market distribution chain.

CONTENTS

1. Introduction 4
   1.1. Cybercrime and Financial Cybercrime 4
   1.2. Stock Market Cybercrime 5
   1.3. Review of Existing Literature 8
   1.4. Scope, Plan and Exclusions 9
2. Cost of Cybercrime 10
   2.1. Uncertainties 10
   2.2. Macro estimates 11
   2.3. Impacts on listed companies 14
   2.4. Cost of financial and stock market cybercrime 16
3. Cyber Insider Trading 17
   3.1. Cases 17
      3.1.1. Information Provider 18
      3.1.2. Bank 20
      3.1.3. Law Firm 20
      3.1.4. Stock Market Regulator 20
      3.1.5. Stock Exchange 22
   3.2. Perspectives 23
      3.2.1. Dark Web and Insiders 23
      3.2.2. Cyberattacks as Inside Information 24
      3.2.3. Data Leaks, a Future Hotbed of Cyberattacks 24
      3.2.4. Sensitive Economic Indices and Indicators 25
      3.2.5. New Entry Points 25
4. Cyber Price Manipulation 28
   4.1. Cases 28
      4.1.1. Intrusion into Retail Trading Accounts 28
      4.1.2. Theft of Personal Data and Dissemination of False Information 29
      4.1.3. Intrusion into Professional Trading Accounts 30
      4.1.4. Organised and Sophisticated Cybercriminal Groups 31
   4.2. Perspectives 32
      4.2.1. Intrusion into Trading Accounts and Mobile Applications 32
      4.2.2. Algorithms 33
5. Cyber Dissemination of False Information 34
   5.1. Cases 34
      5.1.1. The Vinci Galaxy 34
      5.1.2. Dissemination of False Information by Twitter 40
      5.1.3. Dissemination of False Information by EDGAR 43

5.2. Perspectives 44
5.2.1. Very Wide Scope 44
5.2.2. Fake Data 45
5.2.3. Deepfake and Artificial Intelligence 45
6. Cyberattacks on Stock Exchanges 47
7. Stock Market Cybercrime and its Aggravating and Mitigating Factors 49
8. Conclusion 50

1. Introduction

In the 13th edition of its report on global risks in 2018,[1] the World Economic Forum ranks the two risks of cyberattacks and massive data theft/loss among the five major risks in terms of their likelihood of occurrence, alongside environmental risks such as natural disasters, extreme weather conditions and climate change risks, and in sixth place in terms of severity after weapons of mass destruction (sic!), environmental risks and water shortage crises.

1.1. Cybercrime and Financial Cybercrime

More generally, the paradigm shift over the past two decades has been to no longer consider cyber risk as one specific risk among many (somewhere between IT risk and operational risk), but rather as a much more generic risk, or even as a metarisk.[2] This is because, in today's world, everything has become digital, connected, and therefore potentially subject to IT attacks. The digital age has, on the one hand, enabled the renewed use of existing fraudulent schemes and, on the other, paved the way for the emergence of new criminal modi operandi. The term "cyber" is frequently used, in particular to describe any type of crime, whether cyberfraud or cyberterrorism.

There is no commonly accepted legal definition of cybercrime. Nevertheless, the definition[3] borrowed from the inter-ministerial working group for combating cybercrime is suggested here: "Cybercrime consists of all criminal offences that are either attempted or committed against or by means of an information system and communication network,[4] mainly online." The scope is therefore (intentionally) vast. The aim here is not to adopt a legal approach to cybercrime, so we will not dwell on this definition, which varies from one country and one organisation to another.[5] However, we should stress once again that information systems and communication networks can be both the target and the means of illegal behaviour.

In order to limit our scope of investigation, it should be pointed out that we consider cybersecurity as the protection of computer systems from possible cyberattacks, and cyber resilience as the guarantee of the continuity and proper functioning of computer operations in the event of an attack on these systems. As a result, there will be very little discussion of these two concepts, although it is clear that cybercrime, cybersecurity and cyber resilience overlap. More attention will be paid to the modi operandi of cyberattacks than to existing methods of countering them.

Seven years ago, in his speech on 14 September 2011, the Deputy Director of the FBI's Cyber Division[6] outlined the main cyber threats facing the US financial sector. He listed: hacking bank accounts, attacks on payment chain intermediaries, attacks on financial markets by hacking trading accounts or distributed denial-of-service (DDoS) attacks on stock exchanges, credit card theft, attacks on mobile banking services, theft of confidential information, infiltration and/or infection of the supply chain and disruption or jamming of telecommunications networks.

[1] See bibliography [1].
[2] See bibliography [161].
[3] See bibliography [2].
[4] NTIC (New Technology for Information and Communication) may also be included.
[5] See bibliography [3] Section I "Definition of cybercrime".
[6] See bibliography [4].

Since then, events in the news have proved him right: in recent years large-scale financial cybercrimes[7] have continued to be reported, such as credit card thefts or the hacking of the SWIFT[8] payment system (see case below). Cyber risk is now considered the number one risk by most financial institutions, particularly banks and financial regulators.

Case: Hacking of SWIFT
Target: Bank
Summary: The cyberattack on the Central Bank of Bangladesh in February 2016 is one of the most famous attacks of recent years for its sophistication, which combined financial and IT know-how, its significant profit and its symbolism: an attack on a key part of the financial world's infrastructure and on a central bank. The investigation showed that cybercriminals had patiently planned the operation, since they had opened their accounts in the Philippines as early as May 2015.[9] They then compromised the Central Bank of Bangladesh's internal network in January 2016 and monitored employee activity for almost a month, using System Monitor (Sysmon), a Windows system service. The cybercriminals were then able to steal the logins and passwords of the bank's employees that used SWIFT. They were then able to compromise servers in the SWIFT Alliance Access application using specific malware to bypass security devices, make transfers and remove all traces of SWIFT transfers made, both in the database and in the mandatory printed order confirmations.[10] By impersonating Central Bank of Bangladesh officials, requests for transfers from this Bank's account at the United States Federal Reserve in New York to accounts in the Philippines were made on 4 February 2016. It was only on 6 February that the paper confirmations of the transfers made were discovered, revealing the extent of the fraud and leading to 30 transactions being blocked on 8 February. At the same time, typing errors in some messages (e.g. "fandation" for "foundation") also raised suspicions at some banks and prevented the transfer of a transaction for €20 million. Four transactions were approved, amounting to €81 million.
Profit/Impact: The cybercriminals' final profit amounted to €81 million involving four SWIFT messages. The attempt involved a total of €951 million over 35 SWIFT messages.

1.2. Stock Market Cybercrime

While the concept of financial cybercrime is fairly easy to grasp, what do we mean by stock market cybercrime, a subset of financial cybercrime?

The AMF is more colloquially known as the "stock market watchdog". It is an independent administrative authority, comprising approximately 450 people, whose missions are to ensure the protection of savings invested in financial instruments, oversee investor information and ensure the proper functioning of the markets. These missions are partly fulfilled through its law enforcement powers, since the AMF has the power to carry out inspections and investigations, which can lead to administrative and disciplinary sanctions.[11] Within the Investigations and Inspection Division, the Investigations Division, led by Laurent

[7] For a more complete and updated overview of cyber incidents affecting financial institutions, see bibliography [162].
[8] SWIFT (Society for Worldwide Interbank Financial Telecommunication) is a private company owned by its members, whose purpose is to operate an international electronic communication network (also called SWIFT) between market participants, including banks, who exchange standardised messages relating to financial transactions (buy and sell orders, confirmations of trade execution, settlement instructions, payment orders, etc.).
Source: https://www.fimarkets.com/pages/swift_reseau_messages.php
[9] See bibliography [5].
[10] See bibliography [6] and bibliography [163].
[11] "After reviewing inspection and investigation reports, the AMF Board decides whether to open sanction proceedings. If it does initiate proceedings, it serves a statement of objections to the person whose conduct is in question and sends the case to the Enforcement Committee for review and ruling. In certain circumstances, the Board may make an offer of settlement to the

Combourieu, has approximately 25 investigators. These investigators, in those cases that are of interest to us in this report, can investigate the following three main stock market breaches:[12]

1. **Insider trading**, which, according to Article L. 465-1 of the Monetary and Financial Code, consists of a person *"making use of inside information by carrying out, for themselves or others, either directly or indirectly, one or more transactions or by cancelling or amending one or more orders placed by this same person before they are in possession of the inside information, involving financial instruments issued by this issuer or financial instruments to which such inside information pertains"*. Inside information is defined according to paragraphs 1 to 4 of Article 7 of Regulation (EU) No. 596/2014, mainly as: *"specific information that has not been made public, which relates, directly or indirectly, to one or more issuers, or to one or more financial instruments, and which, if made public, would be likely to have a material effect on the price of the financial instruments in question or the price of related derivative financial instruments"*.

2. **Price manipulation**, which, according to Article L. 465-3-1 of the Monetary and Financial Code, is: *"the act, by any person, of carrying out a transaction, placing an order or engaging in conduct that gives or is likely to give misleading signals about the offer, demand or price of a financial instrument or that fixes or is likely to fix the price of a financial instrument at an abnormal or artificial level"* and/or *"the act, by any person, of carrying out a transaction, placing an order or engaging in conduct that affects the price of a financial instrument, by employing fictitious devices or any other form of deception or contrivance"*.

3. The **dissemination of false or misleading information**, which is mainly defined by Article L. 465-3-2[13] of the Monetary and Financial Code, is: *"the act, by any person, of disseminating, by any means,[14] information that gives false or misleading indications about the situation or prospects of an issuer or about the offer, demand or price of a financial instrument or that fixes or is likely to fix the price of a financial instrument at an abnormal or artificial level"*.

It is therefore possible to define stock market cybercrime as all stock market breaches with a cyber component, that are, in other words, "either attempted or committed against or by means of an information system and communication network". It is clear that financial markets with their complex technology and interconnectivity are the most likely to fall prey to these stock market cyber breaches. Stock market crime, even more so than other forms of crime, will therefore not be able to escape "cyberisation".

In this regard, in its July 2017 risk mapping,[15] the AMF highlighted the importance of cyber risks by focusing specifically on this subject. Subsequently, on 19 February 2018, it signed a letter of intent with ANSSI[16] for

respondent and thus avoid opening sanction proceedings before the Enforcement Committee. If the investigation or inspection report reveals criminal offences, the Board will forward the case to the Public Prosecutor", according to the AMF's official website.

[12] It should be pointed out that, broadly speaking, the term "offence" should be used only in relation to criminal offences. A breach, sanctioned by the AMF Enforcement Committee, is the administrative equivalent of an offence, sanctioned by a criminal judge. Unlike an offence, a breach of insider trading rules does not require evidence of speculative intent.

[13] But also Article L. 465-3-3: "1° – To provide or transmit false or misleading data or information used to calculate a benchmark index or information likely to distort the price of a financial instrument or asset to which such an index is linked; 2° – To engage in any other behaviour leading to the manipulation of the calculation of such an index".

[14] Article 12(1)(c) of the European MAR Regulation is even more explicit: "whether through the media, including the internet, or by any other means".

[15] See bibliography [7].

[16] The French National Agency for Information Systems Security (Agence Nationale de la Sécurité des Systèmes d'Information – ANSSI) also covers the financial sector as part of a national defence approach (under the Military Planning Law). The financial sector

enhanced cooperation in the area of information systems protection to address the cyber threat to the financial sector. Finally, in its 2018-2022 strategic plan,[17] the AMF drew attention to how important the issue of cybercrime had become and its desire to develop new skills to respond to it. In the AMF's supervision priorities for 2019, the AMF Chairman announced, on 10 January 2019, short thematic inspections on cybersecurity measures implemented at management companies[18], with cybersecurity also being included in traditional inspections.[19] Finally, the AMF participates, generally with the Banque de France and the Treasury Department, in numerous international working groups focused on financial cybersecurity, such as the G7's Cyber Expert Group and the ESRB's European Systemic Group, or ad hoc groups of the Financial Stability Board (FSB)[20] or IOSCO (the International Organization of Securities Commissions)[21], and in the feedback campaigns run by ESMA[22], the AMF's counterpart at the European level, on the possible improvement of EU texts related to financial cybersecurity. At the European level, we also note the significant involvement of the European Central Bank (ECB) with the publication in May 2018 of the TIBER-EU penetration test framework[23] and in December 2018 of its expectations in terms of cyber resilience for market infrastructures.[24]

Other stock market regulators have also reacted strongly to this threat, notably by creating specialised "cyber units". For example, in September 2017, the SEC (US Securities and Exchange Commission), the AMF's United States counterpart, created such a unit within its law enforcement division to deal with the following issues: the dissemination of false information through social and electronic media, intrusions into trading accounts, hacking of inside information, cyber threats related to market infrastructures and trading platforms, breaches related to Distributed Ledger Technology)[25] (DLT) and Initial Coin Offerings (ICOs),[26] and stock market breaches using the Dark Web.[27]

But what are the specific cases that have marked stock market cybercrime? This study aims to document and analyse all global stock market crimes and breaches from recent years that have a strong cyber

is one of the twelve vital sectors of activity (SAIVs) over which ANSSI has national jurisdiction. Within each SAIV, Vital Importance Operators (OIVs) have been appointed (the list is classified as "Defence Confidential").

[17] See bibliography [8].

[18] In this regard, the French Management Association (Association Française de Gestion, AFG) published in October 2018 the results of a survey on the procedures and resources implemented within asset management companies relating to cybersecurity. See bibliography [164].
Séverine Leboucher's Option Finance article of 10 December 2018 entitled "Management Companies Are Arming Themselves Against Cyber Risk" also demonstrates the growing awareness in this sector.

[19] The inspections, which aim to ensure that entities regulated by the AMF comply with their professional obligations, are carried out by the Inspection Division and not by the Investigations Division described above. The short thematic inspections (known as "SPOT" inspections (Supervision des Pratiques Opérationnelle et Thématique – operational and thematic supervision of practices)), as opposed to traditional inspections on a particular market participant, are intended to evaluate the implementation of certain practices by a small sample of participants.

[20] Which published a "cyber lexicon" in November 2018. See bibliography [218].

[21] Which published the very interesting report called "Cyber Security in Securities Markets – An International Perspective" in April 2016 and "Guidance on Cyber Resilience for Financial Market Infrastructures" in June 2016. See bibliography [165] and [166].

[22] This document of 10 April 2019 entitled "Joint Advice of the European Supervisory Authorities (ESMA, EBA, EOPA)" provides an interesting summary of the European texts in force relating to cybersecurity of market participants supervised by these three European regulators, including ESMA. See bibliography [167] Annex C.

[23] See bibliography [219].

[24] See bibliography [220].

[25] Distributed Ledger Technology (DLT) is a digital system that records asset transactions and their details in multiple locations at once. Unlike traditional databases, DLT does not have a reference data repository or a centralised administration function. Blockchain technology, which groups transactions into interconnected blocks before distributing them to all nodes in the network, is probably the best known DLT. Blockchain is the technology used for Bitcoin, for example.

[26] An Initial Coin Offering (ICO) is a fundraising method that works by issuing digital assets traded for cryptocurrencies during the start-up phase of a project.

[27] The Dark Web (sometimes written DarkWeb or dark web) is the World Wide Web content that exists on networks that use the public internet but is only accessible via specific software, configurations or permissions (friend-to-friend peer-to-peer networks, Freenet, I2P, Tor, etc.). The Dark Web forms a small part of the deep web, the part of the World Wide Web that is not indexed by search engines, although the term "deep web" is sometimes misused in reference to the Dark Web.

component, in order to develop an overview of the modi operandi, impacts and future of stock market cybercrime.

1.3. Review of Existing Literature

While there are many studies on cybercrime in general, there is, to our knowledge, very little literature providing a comprehensive and detailed overview of the impact of cybercrime on stock market crime specifically.

In particular, the SEC's "Cyber Enforcement Actions" website,[28] which lists, without analysing them, the recent cases handled by its cyber unit (see above), will feature significantly.

Nevertheless, several sources have already addressed the phenomenon of stock market cybercrime, but often from a particular angle, generally that of the cyber dissemination of false information and, more rarely, that of cyber insider trading or cyber manipulation. Following the Vinci case in November 2016, to which we will return in more detail later, new French publications appeared such as *"Les 3F du HoaxCrash : Fausse donnée, Flash Crash et Forts profits"* by Thierry Bertier,[29] which focuses mainly on the devastating effects of the possibility of disseminating false information via the internet combined with the current rapid reaction times on the financial markets. Gerard Peliks' publication entitled "Cybercrime"[30] also provides a very detailed explanation of the stock market's "pump-and-dump" mechanism,[31] which is based on spam disseminated by botnets. Finally, Frédéric Echenne's article[32] offers an even more generic view of the risks of uncontrolled financial and information flows on the internet.

Similarly, in his article "The New Market Manipulation", the author points out, in one of his chapters on mass misinformation,[33] that traditional price manipulation is now being replaced by new types of manipulation based on mass cyber-misinformation. Thomas Renault in "Market Manipulation and Suspicious Stock Recommendations on Social Media"[34] also shows, quantitatively, that Twitter seems to be an ideal vehicle for disseminating false information to manipulate the share price of small cap companies.

Finally, it is also worth mentioning a very short but recent article entitled "The Future of Financial Crime and Enforcement is Cyber-based".[35] Its title is quite explicit and also highlights, based on a few well-chosen cases of cyber insider trading and cyber manipulation, the importance of the cyber component for the future of investigations.

Given the very nature of the study, which consists of an overview of stock market cybercrimes, other references will also be referred to in subsequent sections.

[28] See bibliography [9].
[29] English translation: "The 3 Fs of HoaxCrash: False Data, Flash Crash and Formidable Profits". See bibliography [10].
[30] See bibliography [10].
[31] See bibliography [11].
[32] See bibliography [159].
[33] See bibliography [12].
[34] See bibliography [13].
[35] See bibliography [14].

1.4. Scope, Plan and Exclusions

While some scams – which could be described as cyber scams as most of them are committed on the internet[36] – may, under certain conditions, fall within the AMF's jurisdiction, in particular fraud relating to investments in diamonds, Forex or, more recently, cryptocurrencies,[37] we will not investigate this type of cybercrime further, as it is more of a traditional scam than a fraud. More generally, all the crime related to cryptocurrencies (intrusion and theft on trading platforms, ICO fraud, price manipulation, etc.), which ultimately merits a study of its own, will not be addressed in this study either.[38]

In order to better understand the issues, we will first try to obtain some quantified estimates of the cost of global cybercrime, since we cannot accurately quantify the cost of stock market cybercrime. We will also analyse, in detail, the methodology used to calculate this cost.

The following four sections will each address the three main types of cybercrime: cyber insider trading, cyber price manipulation, cyber dissemination of false information, and, briefly, cyberattacks on the stock market itself.[39] Actual cases already dealt with by the authorities will be presented, followed by current threats and perspectives.

Before concluding, a summary mapping of stock market cyber breaches will be presented, together with an analysis of the factors driving these attacks in the financial and stock market sector.

It should be highlighted that this entire study was carried out solely based on publicly available data, either cases posted online by (mainly US) judicial authorities or articles in the specialised press on the internet, as evidenced by the bibliographical references. The overview is therefore certainly not exhaustive, especially since many cybercrimes remain undetected or are detected later on.[40] Moreover, since the time taken to investigate is often considerable, the cases presented here are dated and therefore do not necessarily reflect the current state of stock market cybercrime.

Finally, this report is not intended to make recommendations to improve the effectiveness of combating cybercrime or stock market cybercrime.

[36] In this regard, the Ministry of the Interior's report "State of the Digital Threat in 2018" (see bibliography [15]), did not hesitate to include these online scams in its overview of the digital threat.
[37] Scams where, thanks to attractive websites inviting their visitors to invest in these "future" assets, the money invested is never returned.
[38] Even though recent legislative changes, and in particular the PACTE Law adopted by the National Assembly on 11 April 2019, offer a new regime for crypto-assets in France with optional regulation by the AMF. See bibliography [214].
[39] Even though this type of stock market crime does not necessarily fall within the AMF's remit, it would be difficult to exclude it from a study entitled "Stock Market Cybercrime". However, possible cyberattacks on infrastructure related to the stock exchange (such as post-trade processing) will be excluded from the scope. For example, we can refer to the report "*The Evolving Advanced Cyber Threats to Financial Markets 2018/2019*" (SWIFT/BAE System published in November 2017), which summarises some of the risks associated with this infrastructure. See bibliography [168].
[40] We are of course referring to APT (Advanced Persistent Threat) attacks which are assumed to give priority to persistence in systems and therefore also to the ability to remove their traces.

2. Cost of Cybercrime

This subject is interesting for three reasons. Firstly, it emphasises the importance and the scale of this phenomenon. Secondly, one of the most widely used estimation methods for quantifying this cost is the impact on the share price of listed companies caused by a cyber event (an attack or loss of data), which in itself is an extremely important subject for a stock market regulator. Finally, the uncertainties associated with this calculation provide an understanding of the myriad figures that are often very different from each other.

2.1. Uncertainties

Unlike other risks or other forms of crime that may be more easily quantifiable, measuring the precise cost of a cyber event (an attack or loss of data) to an affected company (and even more so the cost of cybercrime as a whole[41]) is problematic for several reasons, including the following:

- The scarcity of available data. The phenomenon has emerged only relatively recently, and current data under-represent it.[42] Many companies that have been victims of cyberattacks have often chosen[43] not to disclose them or disclose them at a later date[44] (because they did not discover them immediately[45]) for fear of consequences to their reputation or share price (see below). Nevertheless, new regulations[46] should encourage victims to be more diligent and transparent in their reporting.
- The lack of a single definition regarding the costs to be taken into account and the difficulty in quantifying certain costs. While direct costs, such as those related to forensic investigations, legal advice, remedial measures and improvements to affected systems, customer support and the potential loss of short-term income, seem known and easily quantifiable, indirect costs, such as reputational damage and the impact that has on revenue, financing and the loss of clients, and those related to rebuilding a new production system or the loss of strategic information, seem more difficult to assess. Moreover, these indirect costs can only be measured retrospectively and often only several years later. According to an IMF study published in 2017,[47] more than 90% of the total cost of a cyber event comes from indirect costs, including nearly 75% of the long-term revenue losses related to the loss of clients. A schematic view of the various costs associated with a cyberattack taken from the study entitled “The Cost of Malicious Cyber Activity to the US Economy”, published in February 2018

[41] In general, the cost of crime to a company is an extremely complex element to calculate. While the tangible costs directly resulting from crime appear quantifiable, the costs of prevention and the societal and justice-related costs seem more difficult to calculate. The estimation methods used also vary. For example, the total cost of crime in the United States in 2016 was estimated at between $690 billion and $3.41 trillion, a range that varies by a factor of five. Source: See bibliography [16].

[42] It is obviously very difficult to obtain an accurate estimate of the number of cybercrimes reported as a proportion of the total number of cybercrimes. Some sources cite only 3% (source: see bibliography [17]), others 13% (source: see bibliography [18]), or 15% (source: see bibliography [19]) or even maximum 20% (source: see bibliography [20]).

[43] It is also possible that for some strategic corporations, security incidents are covered by national defence secrecy and are only forwarded to the ANSSI.

[44] We are of course referring to Uber or Yahoo, whose management of cyberattack reporting has resulted in many doubtful observers.

[45] We are of course referring to APT (Advanced Persistent Threat) attacks which are assumed to give priority to persistence in systems and therefore also to the ability to remove their traces. In 2017, a compromise incident was discovered on average 100 days later (source see bibliography [21]). In 2014, PwC even claimed that 71% of compromise incidents were not even detected (see bibliography [22]).

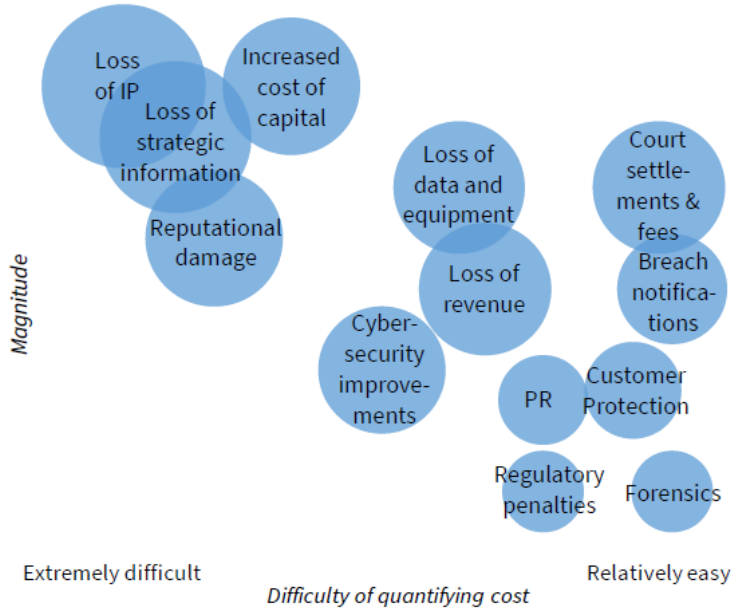
[46] We are of course referring to the new European requirements related to the General Data Protection Regulation in force since 25 May 2018, which requires that the supervisory authority be notified in the event of a data breach; or the SEC’s guidelines in the United States in force since 2011 and revised in 2018, which require disclosure of cybersecurity risks and cyber incidents. See bibliography [169].
In this regard, it is worth highlighting the $35 million fine imposed on Altaba (formerly known as Yahoo!) on 24 April 2018 for not disclosing until 2016 the massive data leak it suffered in 2014. See bibliography [170].

[47] See bibliography [23].

by the United States' Council of Economic Advisors,[48] is reproduced below and illustrates the importance of these indirect costs, which are very difficult to quantify.

- The rapid pace of change in today's technological world and therefore in relation to cyber risk often invalidates the relevance of historical data.
- The heterogeneity of attacks related to cybercrime, both in their scope and variety.

Figure 1. Cost Components of an Adverse Cyber Event



2.2. Macro estimates

According to the latest study by McAfee and CSIS in 2018,[49] the overall range of the cost of global cybercrime increased from between $345 and $445 billion in 2014 (or 0.45% to 0.6% of global GDP[50] estimated at $74.1 billion) to between $445 and $600 billion (or 0.6% to 0.8% of global GDP estimated at $75.8 trillion) in 2017. It is interesting to note that this cost as a percentage of regional GDP is higher and almost identical in the developed regions (North America with 0.69% to 0.87% of GDP, Europe and Central Asia with 0.79% to 0.89% of GDP, Far East and Pacific with 0.53% to 0.89% of GDP), which account for more than 80% of global GDP, and much lower in the other regions (South Asia, Latin America and the Caribbean, Middle East and North Africa, Sub-Saharan Africa).

According to the aforementioned 2018 study entitled "The Cost of Malicious Cyber Activity to the US Economy", the cost of cybercrime in the United States is estimated at between $57 and $109 billion, or 0.31% to 0.58% of GDP. It is therefore already clear that these estimates differ from those presented in the McAfee and CSIS study, which range from 0.69% to 0.87% of GDP for North America and therefore probably apply to the United States.

Applying the lowest (0.31% of GDP) and highest (0.89% of GDP) estimates to France, whose GDP in 2017 was around $2.584 trillion, the overall cost of cybercrime would be between $8 and $23 billion. Other

[48] See bibliography [17].
[49] See bibliography [24].
[50] Gross Domestic Product.

estimates have been circulated, including $7.1 billion[51] and $4 billion[52] for French companies. Once again, it is clear that while the order of magnitude[53] is the same, the variations are significant.

It is interesting to compare the cost of global cybercrime, firstly, with the cost of other crimes, and secondly, with the positive contribution that "cyber" makes to the development of the global economy:

- A 2011 study by McKinsey[54] estimates that the internet's contribution to global GDP is about 3%, while a 2015 study by the Internet Association[55] estimates it to be 6% of US GDP for 2014. Given that in 2014, the cost of cybercrime was around 0.45% to 0.6% of global GDP and that the US figures are commensurate with global figures, we can estimate the proportion of cybercrime to be 10% of GDP generated by "cyber" activities.
- According to figures provided by Global Financial Integrity in its 2017 report on transnational crime,[56] global drug trafficking in 2014 represented between $426 and $652 billion and was the largest contributor to global organised crime estimated at between $1.6 and $2.2 trillion. The aforementioned 2018 study by McAfee and CSIS estimates that cybercrime is the third most lucrative criminal activity after corruption and drug trafficking, but it is undeniably the one that affects most people. In the United Kingdom, it already ranks as the number one activity in terms of the number of crimes reported.[57] It can therefore be concluded, especially given the exponential growth of the digital economy, that cybercrime is fast becoming the most economically damaging crime.

Finally, forward-looking studies, such as those by Juniper Research in May 2017,[58] claim that criminal data loss alone will cost more than $8 trillion over the next 5 years (or $1.6 trillion per year), due to the explosion of connected objects and their low level of IT security.[59] This implies an annual proportion of global GDP approaching 2% rather than the "traditional" 0.8%. Caution should therefore still be exercised, as the world of IT security still has a commercial interest in inflating the cost. Nevertheless, there is no doubt that the annual growth rate of cybercrime could easily exceed two figures.

It is interesting to examine in depth the methodology used by the 2018 report "The Cost of Malicious Cyber Activity to the US Economy" to obtain its range of 0.31% to 0.58% of GDP, because it purposely uses financial market data to quantify the cost of cybercrime and provides an understanding of the inherent uncertainties of this estimation method and, by extension, most estimates of the cost of cybercrime. The basic premise of this method based on the financial markets is as follows: since the share price of a listed company is supposed to reflect its economic value at all times, any economic damage suffered as a result of a cyberattack can be calculated based on any change in the share price. The methodology involved the following steps:

1. Selecting listed companies that were victims of a cyberattack (or data leak) from January 2000 to January 2017, using a syntax search on the database of financial information provider Thomson Reuters, obtaining a sample of 186 companies affected by 290 cyber events.
2. Defining an observation period of seven days after the dissemination of information relating to the cyber event and a characteristic benchmark (here the "market return") to isolate the impact of the cyberattack on the change in share price. This results in an average decrease of 0.8% in market

[51] See bibliography [25].
[52] See bibliography [26].
[53] In the sense of physical order of magnitude.
[54] See bibliography [27].
[55] See bibliography [28].
[56] See bibliography [29].
[57] See bibliography [30].
[58] See bibliography [31].
[59] For even more alarmist extrapolations, see also the annual $6 trillion predicted from 2021 by Cybersecurity Ventures. Source: see bibliography [32].

capitalisation or a more pronounced average decrease of 1.01% if the study period is limited to 2014-2017.

3. The calculation of the overall cost for all listed companies is done by multiplying this average decrease of 1.01% by the total capitalisation of US stock exchanges ($26.6 trillion at the end of 2017) and by the mean annual probability of a significant cyber event occurring.[60] The result is $37.2 billion. Further refinement is considered here by adding the cost of this damage extending to other economically related companies,[61] i.e. $9.2 billion for a total of $46.5 billion or 0.17% of the overall market capitalisation.
4. This 0.17% is extended to the valuation of all unlisted companies and the government sector to obtain an additional $8.7 billion and $0.4 billion respectively. Finally, we add the cost to individuals, estimated at $1.5 billion according to an estimate by the FBI Internet Crime Complaint Center, to obtain a total of $57.1 billion or 0.31% of GDP, the lower limit of the estimate.
5. This estimate can be revised upwards by trying to take into account the under-reporting of cyber events by companies. By replacing the mean annual probability of an initial significant cyber event of 13.85% with 26.78%,[62] we obtain, by repeating the above calculations, a high estimate of $108.6 billion or 0.58% of GDP.

There are, therefore, several key characteristics of this methodology that may explain the uncertainties surrounding the estimates of the cost of cybercrime:

1. The choice of the so-called market methodology. It is not clear that the “true” cost of a cyberattack on a listed company is fully reflected in the change in its share price, and even less so since the existence of stock market cycles has a major influence on the valuation of equities (their relative price).
2. The selection of the sample of listed companies that are victims of an attack. Over what period? What type of attack? Where is the information available? Is the sample sufficiently representative and unbiased?
3. The choice of the time frame for analysis and the benchmark used to isolate the cyber component in the change in the “gross” share price.
4. The estimate of the average occurrence of a cyber event that must take into account the under-reporting bias of this type of event.

[60] This probability is taken from a 2017 Ponemon report on data loss and is 13.85%.

[61] Drawing on the results of two studies by Scherbina and Schlusche in 2015 and 2016, the authors obtain an additional $9.2 billion (37.2 x (0.8 related companies x 0.32 transfer).

[62] According to a 2014 CSIS study, during the attack on Google in 2010, another 34 listed companies were also attacked. However, only Google had reported the attack. When this 3% of actual reporting is compared to the 34 cyber incidents actually reported by companies to Reuters in 2016, there were potentially 1,156 victim companies in total in 2016, which is 26.78% of the total number of listed companies.

2.3. Impacts on listed companies

According to a 2017 study conducted jointly by the specialist company CGI and Oxford Economics,[63] an analysis of the stock market performance of 65 companies, in all sectors and on all continents, that suffered "severe" or "catastrophic" data leaks (according to the Gemalto Index) from 2013 to the first half of 2016 shows that they lost an average of 1.8% of their market capitalisation during the week after disclosure, when compared with a benchmark of their peers.

The 2018 study entitled "The Cost of Malicious Cyber Activity to the US Economy" shows, within the same time frame, an average decrease of 1.01% in the share price compared with the rest of the market (see above).

Similarly, in their study "What is the Impact of Successful Cyberattacks on Target Firms?",[64] the authors, for a final sample of 165 cyberattacks over a period from 2005 to 2017, found an average decrease in company share prices of 1.1% compared with the rest of the market within five days of the announcement.

The Ponemon Institute and Centrify study, from May 2017,[65] on a sample of 113 companies, found an almost instantaneous average drop (consistent with a week of observation but not explained in the study results) and an absolute drop (no benchmark) of 5% of the share price after disclosing a material data breach (defined as a leak of more than 50,000 data records). Nevertheless, most companies seem to recover their original stock market share price within 45 days.

Finally, in the article "Do Firms Underreport Information on Cyber-Attacks? Evidence from Capital Markets",[66] the three authors, by examining a sample of 276 cyberattacks between 2010 and 2015, find that the share prices of companies that immediately report being the victim of a cyberattack fall by an average of 0.7% (but not statistically significantly different from 0[67]) in the month following the announcement (including 0.3% within three days), while the share prices of companies whose cyberattack is revealed by a third party fall by up to 3.56% in the month following the disclosure (including 1.5% within three days). The authors also support the intuitive sense that companies tend to reveal only "small-scale" attacks to preserve their reputational capital.

Once again, the heterogeneity of the criteria selected (in terms of the choice of attacks, the benchmark used, the time frame and study period, the reporting of the attack by the company, etc.) and the small amount of data sampled do not allow a clear conclusion to be drawn. Nevertheless, the range seems to be an average negative impact[68] of between 1 and 5% once a cyberattack is reported.[69]

[63] See bibliography [33].
[64] See bibliography [34].
[65] See bibliography [35].
[66] See bibliography [36].
[67] This could be explained by the fact that before 2014, cyber risk was not yet really taken into account by the market (see bibliography [17] p. 10).
[68] We emphasise "average" here. Consider, for example, Equifax with an 18% drop in just four days (source: see bibliography [37]) or certainly Uber, even though Uber is not a listed company.
[69] Therefore, a final estimate of the cost associated with cybercrime, if based on the so-called market method, may vary by a factor of 1 to 5.

With the global havoc wrought by the NotPetya wiper[70] in June 2017, it may prove useful to obtain the accounting data of the affected companies, when they report it, and compare this data with the theoretical results related to the change in the share price that are described above. For example, we were able to collect the following data on the five companies[71] shown in the table below:

Company	Impact	2017 Results	Ratio
Saint Gobain	€250M less turnover	Turnover of €40.8B	0.6%
	€80M less operating profit	Operating profit of €3.028B	2.6%
Fedex	$215M less profit	Gross operating profit of $5.037B Turnover of $60B	4.2%
Maersk	€250-300M less profit	Cash flows from operating activities of €2.6B Turnover of €31B	11.5%
Mondelez	$103M loss in sales	Turnover of €25.9B	0.4%
	$84M additional expenses	Gross operating profit of $3.5B	2.8%[72]
Merck	$260M loss in sales in 2017 $125M loss in Gardasil sales $200M loss in sales in 2018	Turnover of €40B	1.4%
	$285M additional expenses	Pre-tax revenues of $6.5B	5.8%[73]

It can be seen from the table that the approximate impact ratio on annual operating profit ranges from 2.6% to 11.5%. While the sample is very small with very heterogeneous companies and the specific nature of the PETYA event prohibits any extrapolation, it is nevertheless remarkable to note that by assuming a "price-to-earnings" ratio of about 15, which allows us to convert a company's profit into its market capitalisation, we obtain an estimate of the impact on the share price of approximately 0.5%,[74] which is comparable with the 1% previously mentioned. This would therefore tend to validate the market method.

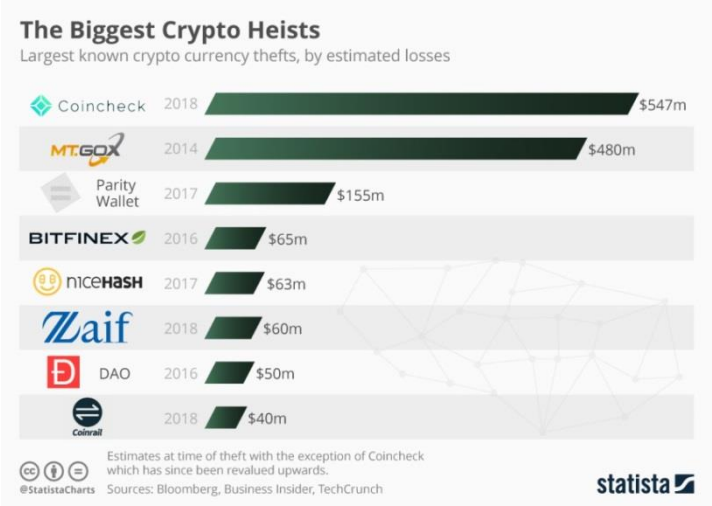
The increase in the number and intensity of cyberattacks, the renewed attention of investors and the public in this regard, the introduction of new laws[75] requiring the reporting of cyberattacks or personaldata leaks with extremely significant financial penalties,[76] and the need to develop cyber

[70] The Petya, or rather NotPetya, virus of June 2017, which should not be confused with the PETYA ransomware of March 2016, was not ransomware but a wiper (from the verb "to wipe" meaning "to clean" or "to erase"), a virus whose only purpose is to destroy data altogether and render systems inoperable.
[71] See bibliography [171].
[72] Taking into account very approximately the impact of the $103 million loss in sales as well as $14 million less profit.
[73] Taking into account very approximately the impact of the $585 million loss in sales as well as $95 million less profit.
[74] The impact on the share price of the company suffering the attack is estimated by dividing the impact ratio divided by the price-to-earnings ratio.
[75] For an overview of these laws, see bibliography [38].
[76] Consider the maximum fines imposed for non-compliance with the GDPR, in force since 25 May 2018, which could amount to 4% of the company's worldwide turnover, i.e. a year of dividends. The total turnover of CAC40 companies in 2016 amounted to €1.2 trillion and dividends paid amounted to €54.3 billion (or 4.5% of the turnover). Also worth mentioning is the $35 million fine (transaction) imposed by the SEC on 24 April 2018 on Altaba (formerly Yahoo!) for failing to report cyberattacks in 2014 (source: see bibliography [39]) and the $700 million fine imposed by the Federal Trade Commission (FTC) on Equifax (see below) for violating US privacy laws (source: see bibliography [216]). In a slightly different context, we should also mention the record fine of $5 billion still imposed by the FTC on Facebook for Cambridge Analytica's use of the personal data of more than 50 million users without their knowledge (source: see bibliography [217]).

insurance[77] are likely to lead to an explosion in data[78] on cyberattacks that will provide a better understanding of the phenomenon and a more detailed assessment of their impact on listed companies.

2.4. Cost of financial and stock market cybercrime

While it seems to be accepted that financial institutions, and in particular banks, remain the main target of cybercriminals, as money is more readily available,[79] it is difficult to obtain a more detailed estimate of the cost of financial cybercrime in and of itself. In order to show the importance of the sums involved, however, it is worth mentioning the recent "exploits" of the group called FIN7, which reportedly stole more than $1 billion using stolen credit cards over 5 years,[80] the "hacking" of the SWIFT payment system, which reportedly yielded more than $100 million[81] for the hackers through six known transactions including the $80 million transaction targeting the Central Bank of Bangladesh, and the attacks on cryptocurrency exchanges, which totalled nearly $1.5 billion at the end of September 2018, as shown in the graph below entitled "The Biggest Crypto Heists".[82]



It is even more difficult, given the narrow scope of the definition of stock market cybercrime, to estimate the cost of this, although the cases presented in later sections may provide an order of magnitude.

[77] The hearing on 15 May 2019 on cyber risk in the economic and financial fields before the Senate Finance Committee of Christophe Delcamp, Deputy Director of General and Liability Insurance at the French Federation of Insurance (FFA), clearly shows that the level of premiums for cyber insurance in France (€80 million) remains very limited in relation to the risks (between €10 and €20 billion estimated for 2018) and that the challenges of quantifying cyber risk are highly specific.

[78] In the bibliography [20], the application of the GDPR already seems to have resulted in the Data Protection Commission (DPC) obtaining 1184 reports in one month, compared with a monthly average of 230 previously, a fivefold increase.

[79] In the bibliography [40] p. 20, the financial services sector pays the highest cost in terms of cybercrime. In the bibliography [24] p. 9, banks remain the favourite targets of experienced hackers. In the bibliography [17] p. 20, the financial sector is by far the most affected by number of attacks in 2016.

[80] See bibliography [42], [43] and [44].

[81] See bibliography [6].

[82] See bibliography [172].

3. Cyber Insider Trading

As defined above, inside information is specific, non-public information that is likely to have a material effect on the issuer's share price.[83] However, what could be more natural for a cyberattacker than stealing confidential information stored in computer systems? Once in possession of this information, it is very easy to monetise it, either by buying the shares before the share price increases once the information has been made public, or by selling it[84] on the black market or on specialised forums on the Dark Web.

Depending on the type of inside information involved, one or more stakeholders may hold it. For example, in the very particular case of so-called "biotech" companies, whose market valuation often depends heavily on the approval given by the regulatory agencies to sell the drugs they have developed, any information held by these regulatory agencies can potentially be inside information.[85]

In the more traditional context of preparing a merger and acquisition (M&A) transaction[86] between an acquiring company and a target company, a whole chain of market participants will potentially be aware of it: the acquiring company, consulting banks, law firms, dataroom providers,[87] accounting firms, consultancy firms, stock market regulators, financial information providers, public relations agencies, potentially translation agencies (in the case of an international transaction), or even the stock exchange itself.[88] Cybercriminals will waste no time in testing the entire chain to identify the weak link as a target.

Most of the cases examined below demonstrate that the threat has the potential to affect each of these stakeholders.

3.1. Cases

Case: FIN4
Target: Issuers
Summary: The FIN4 case is undoubtedly one of the most emblematic of cyber insider trading. By mid-2013, the FIN4 group, as it was named by FireEye in its detailed 2014 report entitled "Hacking the Street? FIN4 Likely Playing the Market",[89] had reportedly targeted more than 100 companies, most of them in the health and pharmaceutical sector, within the aim of hijacking access to the email accounts of these companies' senior managers to extract confidential information relating to potential M&A transactions.
Method: Their intrusion technique was simple although based on a very elaborate phishing scam. No malware was used, but simple VBA macros in documents attached to the phishing email displayed realistic pop-ups asking the targeted person to enter their Outlook login and password. As a way of legitimising

[83] Even though it is outside our scope here, we could also raise the issue of the nature of inside information in a world increasingly dominated by "data scientists" and "big data". If, for example, the analysis of satellite images or the use of drones means that the number of trucks leaving a company's factories and therefore its exact production can be obtained in near real time, and that the anticipated fluctuations in its sales can be extrapolated from this, is this truly inside information? See bibliography [173].
[84] It is not necessarily a cyberattacker that sells on your inside information either; an internal employee can also sell your inside information, which they may have obtained much more easily or with much less computer intrusion. This is the concept termed "insider risk" in the English-speaking world.
[85] See bibliography [174].
[86] For a broader discussion on cybersecurity and M&A deals in general, see FireEye's article "Unsealing the Deal: Cyberthreats to Mergers and Acquisitions Persist In a Hot Market" (bibliography [46]).
[87] In the context of an M&A transaction, the "dataroom" refers to the place where all the legal, tax, accounting and economic documents of a company are made available to potential buyers and their advisers to carry out their due diligence, with the aim of assessing the company's actual situation and the value of its assets.
[88] Some stock exchanges do in fact have a repository that centralises official press releases sent by issuers before making them public. It all depends on the exact path for disseminating information.
[89] See bibliography [47].

this email, the contents of which demonstrated FIN4's intimate knowledge of the financial and business world, the sending addresses used were often real email addresses from previously compromised companies in the same sector of activity, and the documents used were real documents from the target companies that had also been previously stolen.
Profit: It appears that the SEC took an interest in this case as the result of a Reuters article dated 24 June 2015.[90] However, to date, neither the results of this investigation nor the profit made appear to be known.

Case: IT Technician at Expedia[91]
Target: Issuer
Summary: From 2013 to 2016, Jonathan Ly, an IT technician employed by Expedia, committed several breaches of insider trading regulations by compromising the computers and email accounts of several Expedia senior managers in order to steal confidential information relating to the company's financial results. Ly then used this inside information nine times to buy or sell Expedia shares in advance of the official public announcements made by the company and thus make a profit.
Profit: Approximately $350,000.
Method: As a IT technician, Ly enjoyed certain administrative rights. He used these rights to compromise a senior IT technician's workstation, which contained a list of passwords including those for accounts with "super administrator" rights. He then used these to access the emails and computers of the Investor Relations Manager and the Chief Financial Officer, from other employees' sessions to hide his identity. Expedia email accounts and computers continued to be compromised by Ly after his resignation in April 2015, because he had kept one of the company's laptop computers, which continued to allow his remote access.

While the following case is not strictly speaking a theft of inside information in the financial and legal sense of the term, it is very similar and highlights once again the possibility and reality of cyber intrusions into issuers' systems for the purpose of stealing confidential and/or inside information. From 2008 to 2018,[92] two Chinese hackers, members of the APT10 group, were also reported to have stolen confidential information and trade secrets from more than 45 different US companies, before being recently convicted. While it is more likely that they were motivated by state-sponsored industrial and economic espionage, there is no reason, based on this information, to exclude a more economic incentive using insider trading.

3.1.1. Information Provider

Case: Lohmus[93]
Target: Information Provider
Summary: In 2005, two employees of a Ukrainian investment firm Lohmus Haavel & Viisemann (Lohmus) fraudulently accessed the secure website of the financial information provider Business Wire to steal 360 financial press releases that had not yet been made public and, so as to profit from that information, carry out insider trading on the financial markets in over 200 securities.
Profit: €7.8 million.
Method: The two criminals first registered their company Lohmus, in the normal way, as a client of the Business Wire Connect website. This website allowed client companies to send their advance press release

[90] See bibliography [48].
[91] See bibliography [49].
[92] See bibliography [175] and [176].
[93] See bibliography [50].

with the expected time of public release to the media by Business Wire. The two accomplices then authenticated themselves regularly (every two hours) on the website and used an automated "spider" computer program[94] to retrieve and steal all the advance press releases sent by client companies on this site. The two criminals were located and thwarted in particular because they used the same IP address[95] for their financial transactions and for authenticating themselves each day on the Business Wire Connect website used to extract the inside information.

Case: Ukrainian Hackers Compromise Information Providers[96]
Target: Information Provider
Summary: This is one of the most emblematic cases due to its complexity, the degree of professionalism of those involved, its scope and the profit generated. Between 2010 and 2015, two Ukrainian hackers, Ivan Turchynov and Oleksandr Ieremenko,[97] broke into the computer networks of two financial information providers (MarketWire and PRN) and stole almost 100,000 announcements of company financial results before they were publicly released. Turchynov and Ieremenko even created a secret server on which traders could express their wishes regarding announcements to be obtained in the future and shopping lists based on announcements already obtained. The associated traders were based in some 30 different countries (including Russia, Ukraine, Malta, Cyprus, France and the United States) and used this inside information to trade in the shares, options and other financial instruments of a dozen different companies that resulted in a financial gain that they shared with the two hackers (even giving them access to trading accounts as a token of their good faith).
Profit: Profits generated were in excess of $100 million.
Method: The methods used and identified by the investigation were:
- Attacks using a combination of phishing and SQL injection
- Persistent backdoor access
- Interfering with their identity by using the logins and passwords of employees, using malicious codes to erase any trace of their attack and anonymising their IP address.

The above case also illustrates the existence of very sophisticated and well organised insider trading networks (see below).

Case: Oakes[98]
Target: Information Provider
Summary: Between January 2012 and February 2016, Mr Oakes, an IT consultant, accessed, without authorisation, confidential information stored on a computer belonging to a financial information provider in Melbourne consisting of share purchase recommendations made by financial analysts and used it to purchase, on 70 occasions, shares in 52 different companies on the ASX (the Australian lead index) before selling them at a profit once these recommendations had become public.
Profit: Unknown.

[94] A spider is an alternative name often used for a crawler, both being a program that automatically lists and extracts the information contained on a website. See bibliography [51] for examples of spiders. In this case, it is reasonable to assume that the spider used could also search for hidden files and websites by adding appropriate extensions to the addresses found.
[95] An IP (Internet Protocol) address is an identification number assigned permanently or temporarily to each device connected to the internet.
[96] See bibliography [52], [53], [54] and [55].
[97] For a more exhaustive but perhaps also more romanticised version of their adventures, see bibliography [177].
[98] See bibliography [56].

3.1.2. *Bank*

Case: RIVAS[99]
Target: Bank
Summary: From August 2014 to April 2017, an individual named RIVAS breached his duty of confidentiality towards the corporate and investment bank that employed him as an IT consultant in its Research and Capital Markets Technology Group by repeatedly acquiring inside information from the bank's deal/transaction tracking system (M&A or takeover opportunities) and disclosing this information to friends who used it to buy shares in more than 25 companies and then sell them at the most opportune time to make a profit.
Profit: More than $5 million.

3.1.3. *Law Firm*

Case: Chinese Hackers and US Law Firms[100]
Target: Law Firms
Summary: Between March and September 2015, three Chinese hackers penetrated the internal computer networks of two prominent New York law firms to steal inside information about M&A transactions from lawyers' emails and use this information to trade on the financial markets. Two of these hackers also tried, unsuccessfully, to penetrate another five law firms more than 100,000 times.
Profit: Approximately $3 million.
Method: The hackers first compromised the account (login and password) belonging to an IT technician. Using this account, they then penetrated the law firm's internal network and uploaded malware to their servers that allowed them to compromise another account, this time belonging to an IT technician with super administrator rights, and thereby gain access to all of that firm's messaging systems. To avoid detection, the malware was specifically labelled as a Google Chrome update service, and the large download of stolen emails was hidden to appear as normal network traffic.

3.1.4. *Stock Market Regulator*

Case: Intrusion into the SEC's EDGAR System
Target: Stock Market Regulator
Summary: On 20 September 2017,[101] the SEC reported an intrusion into its EDGAR[102] regulatory reporting system dating back to 2016. This intrusion is believed to have more specifically concerned "test filings" (used, for example, when a reporting company needs to check that its financial results submission is in the correct format before submitting a definitive version). The attackers were then able to gain unauthorised access to confidential and non-public information, which could serve as a basis for insider trading. This intrusion was detected by an audit commissioned by the SEC Chairman as part of a more comprehensive plan for cyber security.

[99] See bibliography [57].
[100] See bibliography [58].
[101] See bibliography [59].
[102] EDGAR (Electronic Data Gathering, Analysis and Retrieval) processes 1.7 million electronic regulatory filings per year.

The investigation, which was still ongoing on 21 June 2018,[103] was recently concluded, with the SEC charging the Ukrainian hacker Ieremenko on 15 January 2019[104] with hacking into the EDGAR database to steal more than 157 financial results between May and October 2016, allowing his accomplices – traders based in California, Russia and Ukraine – to generate substantial profits. Ieremenko had already been convicted in 2015 for breaking into the computer networks of two financial information providers, MarketWire and PRN (see above).
Profit: More than $4 million.

This case is certainly very ironic, since the cybercriminals used the SEC as a source of inside information, but it shows once again that cybersecurity must be the priority of all market participants in the financial chain.

The following cases are not strictly speaking cyberattacks aimed at stealing inside information (or at least these cases have not yet been characterised as such), but they all involve potential attacks and/or data leaks that could have been used for this purpose.

Case: Oklahoma Stock Market Regulator Data Leak
Target: Stock Market Regulator
Summary: In January 2019,[105] computer security researchers discovered, using the SHODAN tool,[106] servers containing confidential data belonging to the stock market regulator in Oklahoma state (the "Oklahoma Department of Securities" or "ODS") that had been freely accessible since 30 November 2018. The leak involved more than three terabytes of personal data of all kinds, dated from 1986 to 2016, including emails, regulatory filings, logins and passwords of ODS employees, investigation files (including investigations conducted by the FBI), and so on.
The ODS withdrew public access to these servers the day after the researchers notified it of the issue, and a forensic investigation is ongoing to determine who had access to which document.

Case: FIN7 Spoofs the SEC's Identity
Target: Stock Market Regulator
Summary: In March 2017,[107] FireEye reportedly discovered a targeted phishing campaign by the FIN7 group targeting individuals at 11 listed companies who were responsible for regulatory filings on the SEC's EDGAR platform. The sending address used in the phishing email (EDGAR <filings@sec.gov>) was spoofed to look like the platform's real email address, and a malicious Word document called "Important_Changes_to_Form10_K.doc" was attached to it. When opened, this document used a VBS script to install a PowerShell backdoor (called Powersource by FireEye) using DNS TXT queries as a communication channel to FIN7's control centre. The purpose of these attacks is still unknown.

Another case involving a fairly similar attack, which could also be the work of the FIN7 group, was identified by Cisco-Talos (below):

[103] See bibliography [60].
[104] See bibliography [178], [179] and [160].
[105] See bibliography [180].
[106] SHODAN is a search engine created in 2009 by John Materly that references the results of large-scale port scans performed on the internet. Thanks to its numerous filters, it can be used to find specific connected objects (routers, servers, web cameras, industrial control systems, etc.) and detect certain vulnerabilities (such as the absence of a password or the use of default passwords). For a simple overview of this tool, see bibliography [181].
[107] See bibliography [61] and [62].

Case: SEC's Identity Spoofed Again
Target: Stock Market Regulator
Summary: In October 2017, Cisco-Talos[108] uncovered a new version of a DNSMessenger attack[109] that used phishing emails that impersonated the identity and colour schemes of the SEC and its EDGAR regulatory filing database. These emails contained infected Microsoft Word documents that also seemed official (with the SEC colour scheme and graphics, etc.). When opened, these documents asked victims to authorise the activation of links to download external files, which was required to display the document in its entirety. If victims gave their authorisation, malicious code was downloaded and the malware infection began. These highly personalised, complex attacks, with the use of numerous scrambling techniques, seem to indicate a sophisticated, motivated and persistent attacker. But the purpose of these attacks is still unknown.

A similar attempt to spoof the AMF's identity in a targeted email campaign (email address ending @amf-fr.org instead of @amf-france.org), inviting recipients to download a Word document containing malicious content, was also reported by the AMF on 19 October 2018.[110] An article in the *Times of Malta* on 25 February 2019[111] suggested a possible link between this targeted email campaign spoofing the AMF's identity and the cyberattack on the Bank of Valetta (Malta), resulting in a profit of €13 million for the attackers.

Unfortunately, this type of attack, spoofing the identity of a regulator to send infected emails, seems quite widespread, as the Australian counterpart to the AMF – the Australian Securities and Investments Commission (ASIC) – has also been attacked.[112]

More generally, email-based attacks ("phishing" or "spearphishing"), are well known in the IT security world, and, even though the tactics change and become more diverse, they remain one of the methods most favoured by hackers,[113] especially in the financial world.[114] They are simple to implement, inexpensive and allow attackers to easily target the human factor, a weak link in any organisation, while at the same time delivering extremely sophisticated malware.

3.1.5. Stock Exchange

Case: Nasdaq OMX[115]
Target: Stock Exchange
Summary: In February 2011, it was revealed that cybercriminals had successfully compromised an application of the Nasdaq OMX stock exchange called "Director's Desk". This application allowed information to be shared between members of the boards of directors of listed companies (more than 300 companies). This information is largely inside information. The cybercriminals did not appear to succeed in compromising the "market" part of the stock exchange, only this one application. There has been considerable speculation about the true nature of this incident.

[108] See bibliography [63] and [64].
[109] This is an attack that uses DNS TXT exchanges to communicate between the infected computer and the attack control centre (see bibliography [65]).
[110] See bibliography [182].
[111] See bibliography [183].
[112] See bibliography [184].
[113] See bibliography [185].
[114] According to a PhishLabs report on phishing campaigns in 2018, financial institutions are among the most affected organisations and represent nearly 29% of those targeted. See bibliography [186].
[115] See bibliography [66] and [67].

3.2. Perspectives

3.2.1. Dark Web and Insiders

In the cases above, we have seen that the monetisation of stolen inside information was achieved directly through its use on the financial markets. However, since cybercrime offers its own services, the monetisation of this inside information can also involve it being sold on the Dark Web.

In RedOwl's 2017 report "Monetizing the Insider",[116] the authors argue that the Dark Web is increasingly being used by cybercriminals to purchase inside information. This information often comes from employees of the company to which the inside information pertains. The Dark Web is also used to directly recruit these internal company employees (known as "insiders"[117]), who can provide cybercriminals with access to the company's internal computer network or even help them introduce malware. Activity on the Dark Web, measured in terms of the number of posts relating to the aforementioned themes, is estimated to have doubled between 2015 and 2016, and two examples of very active forums that claim to be very demanding in terms of the quality of the information gathered, with evocative names such as "Kick Ass Market Place" or "The Stock Insiders", allegedly provide inside information that can be monetised on the stock market.

It should also be emphasised that, even though some of the information available on the Dark Web is not inside information per se, it can provide one of the building blocks required for cyber insider trading. For example, a British IT security company, in its January 2018 report entitled "Securing the Law Firm: Dark Web Footprint Analysis of 500 UK Legal Firms",[118] showed that each of the 500 largest British law firms had on average 2,000 email addresses with passwords available on the Dark Web. Most of this data comes from a third-party data loss, where we imagine employees of these law firms have registered with their professional email address and a password on a third party's website. This data may be the source of a targeted and relevant phishing attack on the law firm employee who owns the email address in question or of a "credential stuffing" attack.[119] Finally, if the information already on sale on the Dark Web is not sufficient, it seems that, according to some articles,[120] a hacker can be hired directly "à la carte" to compromise a potential target's personal or professional email account or social media account.

Therefore, although it is difficult to know the full extent of inside information (in the stock market sense) available on the Dark Web, it seems justified for stock market regulators to arm themselves at the very least with search engines capable of exploring the Dark Web, in order to review and monitor the information it holds. However, they are often not legally authorised to use the undercover techniques needed to do this in the forums, and some sources argue that the Dark Web is becoming less attractive, losing out to media such as Telegram.[121]

---

[116] See bibliography [68].

[117] On the concepts of insider and insider risk, which have gained more attention in recent years, see SIFMA's very comprehensive document "Cybersecurity: Insider Threat Best Practice Guide" (2nd edition, February 2018) (see bibliography [69]).

[118] See bibliography [70].

[119] Credential stuffing is a practice that uses the credentials stolen from an account on a hacked website to try to access several accounts on various other websites automatically (using botnets, in particular). This practice is used to access all those accounts for which the victim of the first hacked account uses the same password.

[120] See bibliography [71].

[121] See bibliography [72] and [73].

3.2.2. *Cyberattacks as Inside Information*

Given the importance of cyber risk for listed companies and, more importantly, its potential impact on their share price (see above), it would be natural to consider cyberattacks not as a means of stealing inside information, but rather as the inside information itself. For example, the SEC recently filed a lawsuit against a senior figure at Equifax who had used the as yet unpublished information from Equifax's massive data leak to sell his shares (see below).

Case: Equifax Senior Executive Commits Insider Trading[122]
Summary: Jun Ying, CIO of Equifax US Information Solutions and expected to become the company's Global CIO, committed insider trading by using his knowledge of a massive (but still confidential) personal data loss suffered by Equifax to sell his stock options, before the company made this cyber incident public in a press release in September 2017. The data leak involved the personal data, such as social security numbers, of 148 million US citizens.
Profit: By selling these stock options at the most opportune time, Ying avoided a potential loss of $117,000.

For the curious reader, a very interesting report from the US Government Accountability Office (GAO)[123] analyses in detail the internal IT failures of Equifax that led to this massive data leak: the existence of a critical vulnerability, the patch for which, released only a few days before, had not been fully implemented; insufficient database segmentation allowing attackers to directly and easily access all data; and the poor configuration of network traffic monitoring equipment, resulting in a 76-day detection time.

While the legal framework is not strictly the same as insider trading, the case of Muddy Waters with St. Jude Medical[124] is also interesting, as Muddy Waters announced publicly that St. Jude Medical's medical devices (including its pacemakers) had serious cybersecurity deficiencies and were vulnerable to cyberattacks (as conducted and recorded by a cybersecurity company that specialised in the medical field). Muddy Waters hoped to take advantage of the drop in the share price caused by the public dissemination of this information to take advantage of its short selling positions on St. Jude Medical.

Therefore, a cybercriminal, having previously sold the shares of a target company, could order a cyberattack (DDoS, ransomware, malware, confidential data leak, etc.) on that company for the sole purpose of benefiting from the fall in its share price at the time the cyberattack is announced.

3.2.3. *Data Leaks, a Future Hotbed of Cyberattacks*

This is not a new phenomenon, but the massive data leaks of recent years (Yahoo, Uber and Equifax among many others, known and unknown) will undoubtedly also be a future hotbed of cyberattacks where criminals will already have half the work done for them. They would be able to use this information to carry out cyber insider trading[125] by monitoring the previously compromised personal (or professional) email account of a senior manager or employee of a listed company, or by spoofing the email address or even stealing the identity of this person, to launch a phishing campaign, which, on the face of it, appeared

[122] See bibliography [74].
[123] The audit, evaluation and investigation body of the US Congress responsible for auditing the public accounts of the federal budget. See bibliography [187].
[124] See bibliography [75].
[125] In the same way, trading account intrusions and the dissemination of false information would also be made easier.

to be legitimate. As an example, in a recent classic case of financial fraud with identity theft,[126] the criminal used personal data from a major data leak that occurred four years ago. In another example, cybercriminals in the Shalon case (see below) used email addresses that they themselves had stolen as targets for their promotional campaign.

3.2.4. Sensitive Economic Indices and Indicators

Economic indicators, indices or data is extremely sensitive data for financial markets. Whoever holds this information in advance of its official publication holds inside information, which of course relates to the financial instrument concerned.

For example, the Michigan Consumer Sentiment Index (MCSI), which is widely observed in the United States for its impact on stock market indices, is calculated by researchers at the University of Michigan[127] and sent to Thomson Reuters, which distributes it to its clients through its own communication channels. The level of (cyber)security upstream of this index is a potential issue. These indicators can be calculated by external private sector organisations, such as the University of Michigan,[128] but also by state bodies. For example, the official unemployment figures in France are calculated by Pôle Emploi (French employment agency) and DARES (French Ministry of Labour's statistical service), and have a significant impact on the valuation of certain listed instruments such as French bonds, the French sovereign CDS[129] or the CAC40 index. It is not certain whether the protocol for producing and communicating all these indicators has considered the possibility of an intrusion into their computer system. A Finnish example from 21 November 2018,[130] involving cyberattacks on an official website hosting potentially sensitive data from the Ministry of Economic Affairs and Labour, shows that these scenarios are not fictional. This is particularly true since much of this potentially sensitive data originates from public bodies, whose IT systems seem to be at particular risk throughout the world, owing to the obsolescence of existing technologies and the upcoming retirement of the managers responsible for maintaining these systems.[131]

These are just a few examples out of many. For each asset class (equities, credit, interest rates, exchange rates, commodities, energy, real estate, etc.), there is a wide range of financial instruments, the price of which varies according to several pieces of data. A more comprehensive mapping exercise at the level of each stock market regulator could be useful in defining the list of key indicators and pieces of data that could be the target of cyber insider trading, depending on the level of security associated with how they are produced and distributed.

3.2.5. New Entry Points

With the proliferation of laptops, smartphones and now connected objects (nearly 8.4 billion in 2017 and almost 20.4 billion by 2020[132]) and the massive migration of businesses to the Cloud, potential entry points

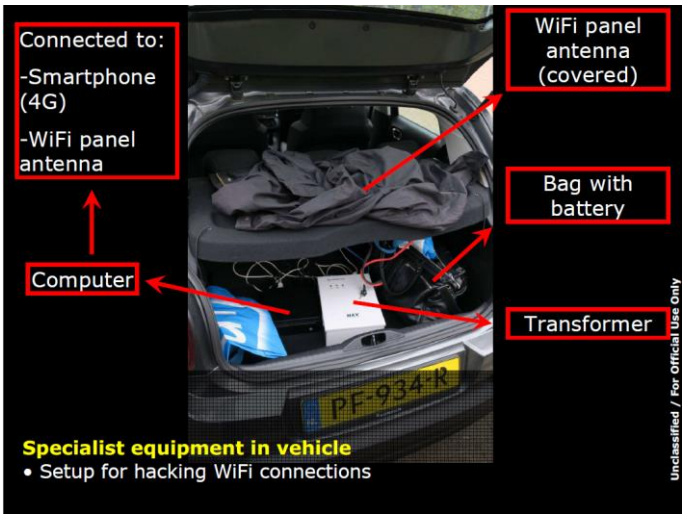
[126] See bibliography [76].
[127] See bibliography [77]. In this regard, Thomson Reuters, in partnership with the University, gave its best clients the opportunity to obtain the renowned index ahead of the others. This practice was subsequently discontinued as it gave an unfair advantage to its best customers, in this case inside information (source: see bibliography [78]).
[128] For example, there is also the Consumer Confidence Index calculated by the Conference Board and the Purchasing Managers' Index (PMI; also called the ISM Index) calculated by the Institute of Supply Management, among many others.
[129] CDS or Credit Default Swap: a credit derivative product used to hedge against the occurrence of a default in payment in exchange for a premium. A higher than expected unemployment rate is likely to increase the premium intended to insure against a default by the French State.
[130] See bibliography [188].
[131] See bibliography [189].
[132] See bibliography [79].

for cybercriminals are increasing: business travellers, particularly senior managers with confidential information, are an ideal entry point for cybercriminals if remote connections are not secure,[133] and for employees whose mobile equipment is used for both personal and business purposes, there is a risk of malware being downloaded from compromised websites or social media platforms.[134] Certain risks such as public/open Wi-Fi network connections, in hotels for example, are also known.[135]

But what about the opportunities created by the new digital behaviours of companies whose services (such as email, especially with Microsoft Office 365) are increasingly centred around the Cloud, often with a single central authentication layer?[136]

What about the possibilities of rapid battery charging in public or other areas using a USB connection?[137] Similarly, there are the vulnerabilities created by connected objects such as smartwatches and other gadgets that we connect to our computers, or voice controlled connected objects, some of which have been found to be able to record conversations without our knowledge.[138] Even expert voice assistants on smartphones are vulnerable to being compromised.[139] The most well-known antivirus software vendors, beloved by IT security systems, are bursting with information about these systems, and the recent controversy[140] over the security risks posed by the Kaspersky products that could have been exploited by malicious Russian cyber actors to compromise US federal information systems is evidence of this.

More generally, all the methods used for cyber espionage are relevant, as evidenced by the Russian spying attempt on 4 October 2018 exposed by the Netherlands,[141] where equipment to intercept Wi-Fi traffic was discovered in the boot of an unmarked car parked near the car park of the targeted building in the Netherlands (see photo below[142]). Such a campaign could also be used to steal inside information.



[133] See bibliography [80].
[134] According to a report by the cybersecurity company Bromium, cybercrime involving social media is on the rise. The report suggests that one in five corporate compromise incidents are related to malware distributed by a social media platform. See bibliography [190].
[135] See bibliography [81].
[136] See bibliography [191] and bibliography [192].
[137] See bibliography [82].
[138] Google Home or Amazon Alexa devices in the offices of senior managers could easily obtain inside information.
[139] See bibliography [83].
[140] See bibliography [193].
[141] See bibliography [194].
[142] See bibliography [195]. The photo shows a covered Wi-Fi antenna on the parcel shelf and, in the boot, a bag with a battery, a transformer and a computer connected to a smartphone (4G) and to the Wi-Fi antenna.

Another example is the controversy of October 2018[143] accusing China of economic espionage against large US companies, whose computer servers had microchips installed in them that were produced in China.

In short, while many players in the stock market world may be targeted by cybercriminals in search of inside information, the intrusion possibilities afforded by new technologies are increasing, and the attack surface is expanding proportionately.

[143] See bibliography [196] and [197].

4. Cyber Price Manipulation

There are many different types of price manipulation. However, to "artificially" manipulate the price of a financial instrument and make its price rising,[144] there are three options, none of which is mutually exclusive:

1) Buy the shares aggressively at increasingly higher prices, which will automatically increase the price (a bit like an auction);
2) Issue buy orders of significant value that are not intended to be executed, to signal a strong buying interest to the rest of the market, thereby leading it to adjust its prices upwards ("layering/spoofing").
3) Spread false rumours aimed at causing the market to speculate upwards on a particular security.

When criminals use strategy 1 and/or 3 ("pump") before selling at a profit ("dump") the securities they previously bought at low cost, they are employing the well-known manipulative scheme called "pump-and-dump".

The potential cyber component is obvious. Compromising trading accounts is a means to implementing strategies 1 and 2, while the vehicle for spreading false information in strategy 3 is largely cyber- or digital technology-based (e.g. emails, fake websites, social media platforms). This third strategy is described in detail in the section on cyber dissemination of false information, even though it may also fall within the scope of cyber price manipulation.

The cases presented here are mainly "pump-and-dump" cases where retail trading accounts have been compromised.

4.1. Cases

4.1.1. Intrusion into Retail Trading Accounts

Case: Willner[145]

Summary: From September 2014 to August 2016, Joseph P. Willner manipulated the price of several equities through transactions made by his accomplice from more than 110 hacked trading accounts to make a profit on his own personal trading account. Willner then shared half of the profit he made with his accomplice. In an instant message exchange between the two scammers, the investigators found the following tagline: **"Legal trading is too hard"**. The two examples below provide an insight into the manipulations they potentially used.

On 10 April 2015, after the market closed, Willner placed a short sale order for 537 shares in First Community Corporation ("FCCO") at a limit price of $14.88 per share, well above the closing price of $11.64. At the same time, his accomplice hacked into a victim's trading account and places a buy order for 537 shares with a limit price of $14.88. The two orders were executed one against the other. A few moments later, Willner placed a buy order for 537 shares at $9.40, well below the closing price of $11.64, and his accomplice placed the opposite sell order on the victim's account. As a result, Willner made a profit of $2,942, while the victim lost this amount.

On 17 May 2016, during trading hours, one of Willner's accomplices used a victim's account to buy a large number of Lawson Products, Inc. ("LAWS") shares at a much higher price, which automatically caused the LAWS share price to increase. Willner then short-sold the shares at this artificially high price while his

[144] The opposite is of course true for a financial instrument whose price is falling.
[145] See bibliography [84].

accomplice used the same victim's account to this time sell the large number of shares previously bought until the share price fell significantly. Willner then bought the shares at this low price and pocketed the difference.
Profit: At least $700,000 for the trader, but a loss of $2 million for the brokerage firms affected.
Method: The methods used to compromise victims' accounts are not known. Willner had taken care to use a pseudonym when using instant messaging with his accomplice on the internet. However, he accessed this messaging service using a real IP address that was tracked to his home.[146]

Case: Mustapha[147]
Summary: In April and May 2016, Idris Dayo Mustapha compromised many retail trading accounts and used them to make a profit on his own personal account. The manipulative scheme is similar to the one presented above, with an aggressive purchase of shares using victims' accounts to set the price at an artificially high level and then sell the shares at a profit using the criminal's account.
Profit: $68,000 in profit for Mustapha and at least $289,000 in losses for the victims.
Method: The accounts were reportedly compromised using an administrator account to access them. But how this administrator account was compromised is not described.

Case: The Latvian Trader[148]
Summary: From June 2009 to August 2010, a Latvian trader, Igors Nagaicevs, manipulated the price of more than 100 shares on the NYSE and NASDAQ, by compromising retail trading accounts. The modus operandi is fairly similar to the previous ones: taking a buy (or sell) position on the trader's personal account, manipulating the price up (or down) by making multiple, aggressive buys from victims' accounts, and finally unwinding the initial position on the trader's personal account with profits from selling (or buying) at artificially high (or low) prices. The trader often managed to make his entire round trip in only 15 to 20 minutes, but he was still responsible (including the victims' accounts) for more than 50% of the daily volume traded. He carried out these manipulations more than 150 times in 14 months.
Profit: $850,000 in profit plus more than $2 million in losses for his victims.
Method: Not disclosed.

Case: BROCO [149]
Summary: From August 2009 to December 2009, Valery Maltsev, President of Broco Investment, manipulated the price of at least 38 shares by compromising retail trading accounts. The modus operandi is identical to that of the Latvian trader above.
Profit: $255,000 in profit for Broco Investment and $600,000 in losses for the victims.
Method: Stolen logins and passwords. The technical means used were not disclosed.

4.1.2. Theft of Personal Data and Dissemination of False Information

Case: Shalon "*Securities Fraud on Cyber Steroids*"[150]
Summary: This case has been called one of the largest cybercrimes in history because of the extent of the fraud. More than 100 million personal data records were stolen from 12 separate financial institutions, including 80 million records from JP Morgan Bank alone. An international network of criminals, with more

[146] Proof that he was an amateur, if it were needed.
[147] See bibliography [85].
[148] See bibliography [86].
[149] See bibliography [87].
[150] See bibliography [93], [94] and [95].

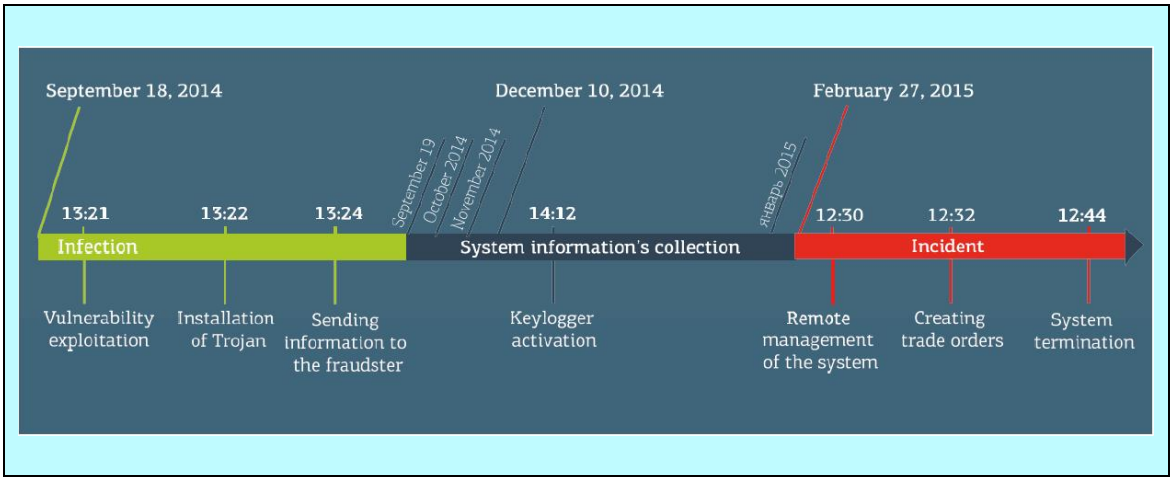
than 30 forged passports of 17 different nationalities, used the theft of personal data to wrongfully solicit future victims by luring them into scams as varied as traditional stock market manipulation schemes like "pump-and-dump", illegal internet casinos and even an illegal bitcoin trading market.
Using at least 20 promotional websites and a large list of email addresses (previously stolen as part of a relatively targeted personal data theft of clients of financial institutions), cybercriminals launched promotional campaigns on a dozen or so equities during 2011 and 2012, sending emails that appeared to come from many apparently different sources that urged retail investors to invest in these equities, while being careful to highlight that they themselves had previously invested in them. Once the excitement around these equities had been built, the criminals quickly sold them, generating a healthy profit.
Profit: More than $100 million in total, including at least $2.8 million from stock market fraud.

This example, of a group whose business model seems to be entirely cyber-focused, once again demonstrates the interest of organised cybercriminal groups in stock market cybercrime. It also demonstrates the risk, already mentioned above, associated with the loss or theft of personal data, which can be exploited in many ways, here with malicious but targeted promotion for the purpose of stock market manipulation.

4.1.3. Intrusion into Professional Trading Accounts

Case: ENERGOBANK/CORKOW[151]
Summary: In February 2015, a cyberattack against the trading systems of a Russian bank took place with unauthorised transactions for a notional amount of around $500 million[152] on the dollar/rouble currency pair, lasting 14 minutes and using Trojan-type malware. These transactions significantly destabilised the normally stable currency exchange rate of 60-62 roubles to the dollar, changing to 55 and then 66 roubles to the dollar for a few moments, before returning to its usual values. The result of this attack was a significant loss of reputation for this bank, and some experts believe that it was only a preliminary test by cybercriminals preparing for a larger scale operation.
Profit: The bank reported losses of $3.2 million. Nevertheless, it should be noted that the exchange rate varied by almost 15% from 66 to 55 roubles to the dollar and that this price also sets the price of all derivative instruments based on this underlying exchange rate, such as CFDs and others. It is therefore not impossible to imagine that accomplices could have benefited from this fluctuation in another market.
Method: To carry out their attack, the criminals used Corkow malware, also known as Metel, which contains modules specific to Russian trading systems.[153] Corkow provides remote access to these trading systems. On 18 September 2014,[154] cybercriminals penetrated the system by exploiting a vulnerability and installed the Trojan, which was regularly updated to avoid detection by the bank's antivirus software that was otherwise functioning normally. Group-IB even claims that in March 2015, no antivirus software was able to detect version v.7.118.1.1 of Corkow. The information gathering phase then began and keyloggers were activated in December 2014. Eventually, on 27 February 2015, remote access was obtained and trade orders were issued. Finally, 14 minutes after the first order was sent, the cybercriminals tried to remove Corkow from the trading system and destroy all traces of its past activity. For a more detailed technical analysis of Corkow malware, see above.

[151] See bibliography [88] and [89].
[152] Nevertheless, only 250 million were ultimately executed.
[153] Such as QUIK by ARQA Technologies (https://arqatech.com/en/products/quik/) and TRANSAQ by ZAO (http://www.transaq.ru/en/).
[154] See the graphic below which details the following events: vulnerability exploitation, installation of the Trojan, sending information to the fraudster, keylogger activation, remote management of the system, creating trade orders, and system termination.



4.1.4. *Organised and Sophisticated Cybercriminal Groups*

The ENERGOBANK case is very revealing for two reasons:

- Stock market cybercrime attracts organised and highly sophisticated cybercriminal groups;
- Attacks can now reach the trading systems used by financial market professionals and not just those used by retail investors, increasing the impact on market integrity.

As the ENERGOBANK and SWIFT cases described above reveal, the sophisticated approach of cybercriminal groups specialising in finance and stock markets is remarkable, as it combines a very high level IT expertise[155] with an in-depth knowledge of financial mechanisms.

While the mapping of cybercriminal groups that specialise in finance is not the subject of this report, we can nevertheless mention the following well-known actors motivated by economic gains (unlike hacktivists), despite the difficulty of separating them into those that are still active and those that are not:[156] Corkow[157], Carbanak (the mastermind behind which was arrested in Spain in early 2018),[158] Cobalt[159], FIN4 (see above), FIN7 (three members of which were also arrested in August 2018),[160] Lazarus[161] (also known as Hidden Cobra, Dark Seoul, APT38), etc.

[155] The CEO of Sophos, Kris Hagerman, notes that the volume and variety of malware continues to grow. One of the major trends is that malware and the tools used to create it are becoming increasingly sophisticated. Hagerman also states that a growing percentage of malware is being developed specifically for attackers' intended targets. As a result, this sophistication is not necessarily the exclusive preserve of nation states, particularly in a context where the boundaries between cybercrime and cyber espionage remain porous. See bibliography [198].

[156] See bibliography [199] and [200].

[157] See bibliography [90].

[158] "The hackers in the Carbanak Group began their attacks at the end of 2013 with their Anunak software, which targeted financial transfers and Automated Teller Machine (ATM) networks of financial institutions. The following year, they released a more sophisticated version of Anunak, known as Carbanak, which was used until 2016. They then launched a wave of even more sophisticated cyberattacks using the Cobalt Strike software, which allowed them to instruct ATMs to dispense cash at pre-determined times." See bibliography [201] and [202].

[159] In their blog (see bibliography [91]), the authors point out that the Cobalt Group mainly targets banks but also all financial institutions, and that it could be particularly interested in stock exchanges, as predicted by the Russian Central Bank's FinCERT. This Cobalt Group still appears to be extremely active (source: see bibliography [92]).

[160] See bibliography [42].

[161] According to this article of 1 April 2019 (see bibliography [203]), the Chinese company 360 Security published a report on the activities of the Lazarus advanced persistent threat (APT) group (also known as Hidden Cobra, Dark Seoul and APT38) on cryptocurrency platforms. The misappropriation of funds has reportedly increased, particularly with the latest compromise of the DragonEX platform in March 2019. By analysing this attack, the researchers identified fake trading software called Worldbit-bot used by the attackers, which was embedded with malicious code and distributed to internal staff at cryptocurrency exchanges under the pretext of offering them a promotion on this software. A backdoor was installed on the staff's computers, allowing attackers to obtain the private key to the wallet and operate on the compromised networks for months.

4.2. Perspectives

4.2.1. Intrusion into Trading Accounts and Mobile Applications

There were some examples of hacking into retail trading accounts in the United Kingdom and France in 2011 and 2016 with modi operandi very similar to those presented above. So far, however, the stakes were not too high and the intrusions were quickly detected.

Nevertheless, according to the Hong Kong local authorities,[162] retail trading accounts being compromised for the purpose of manipulating share prices seems to be a particularly serious problem, not least because of the number of penny stocks listed, the proximity of Chinese hackers and the low level of cybersecurity that brokers have compared with other financial operators and retail banks. At least seven brokers and eight banks, including HSBC Holdings PLC and Bank of China International (BOCI) Securities,[163] have been targeted by such attacks. The phenomenon has become more prominent in recent years, with a tripling of cases in 2016 (81) compared with 2015.

In response, the Hong Kong Securities and Futures Commission (SFC) launched, on 13 October 2016,[164] a cybersecurity review of mobile and/or internet trading systems. After making the consultation with the sector public in May 2017,[165] on 27 October 2017,[166] new guidelines were issued, proposing, inter alia, the implementation of two-factor authentication given the poor security provided by passwords. In view of the constant, rapid changes in habits and technologies in Asia, the Hong Kong regulator has even had to issue guidelines[167] for trading on instant messaging platforms, which are even more vulnerable to cyberfraud than other means of communication. In general, the extremely rapid digitalisation of the Asia-Pacific region,[168] which does not necessarily go hand in hand with a corresponding level of investment in cybersecurity, particularly for SMEs, which are an integral and significant part of the regional economic fabric and can be subcontractors for larger, more international companies,[169] makes it a prime target for cybercriminals.

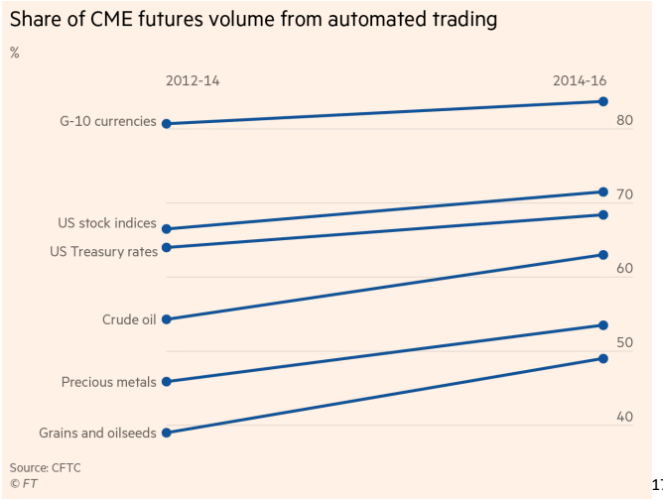
The challenge of securing trading applications and accounts seems to be a much bigger problem than expected. A July 2018 report[170] showed that many trading applications (mobile and desktop) – even among such well-known US players as Charles Schwab, Fidelity, Interactive Brokers and TradeStation – were much less secure than their bank payment counterparts. Some applications were even so insecure that the data sent to the server was not encrypted, allowing attacks such as “Man-In-The-Middle” (MITM) attacks. Nevertheless, the researcher points out that the platforms operated by Bloomberg and Capital One are the most secure.

[162] See bibliography [96].
[163] See bibliography [97].
[164] See bibliography [98].
[165] See bibliography [99].
[166] See bibliography [100].
[167] See bibliography [101].
[168] See bibliography [102].
[169] Consider Target, whose intrusion only happened because of its subcontractor responsible for heating, air conditioning and ventilation (source: see bibliography [103]).
[170] See bibliography [104].

4.2.2. *Algorithms*

Algorithms are at the heart of modern financial exchanges. Depending on the asset classes involved, algorithms were already responsible for at least 50% to 80% of the daily trading of futures contracts on the US-based Chicago Mercantile Exchange (CME) (see graph below) over the period 2014-2016, while on the US equity markets, high-frequency trading, which is a sub-branch of algorithmic trading has accounted for at least 50% of daily trading over the past ten years. If we consider orders issued but not executed, then the incidence of high-frequency trading increases to more than 90%.

We should remember the unfortunate purchase, in the space of half an hour, of several billion dollars' worth of US shares by Knight Capital, a company specialising in high-frequency trading, following an error in one of its computer algorithms (probably a new algorithm released to production[171]) and which cost it more than $440 million, leading to its subsequent merger with Getco, now Virtu Financial.



[172]

It is therefore not difficult to imagine that a cybercriminal, albeit a talented one, could knowingly compromise the algorithms of this type of trading company to manipulate the prices of certain instruments for economic purposes or simply to destabilise the market by sending a series of massive sell orders.[173]

In view of this strong presence of high-frequency trading companies whose profits depend on their speed (their reference unit of time has become the microsecond), and from a conceptual point of view, it is interesting to mention this theoretical manipulation[174] which involves slowing them down by injecting a large amount of superfluous data into the communication channels linking these companies to the stock market. This type of attack on high-frequency algorithms would be equivalent to a denial-of-service (DoS) attack on websites.

Finally, more generally, one could easily imagine a malware attack trying to modify the content of the orders sent by one or more market participants, once they have arrived at the stock exchange.

---

[171] See bibliography [106].
[172] See bibliography [105]. This graph shows, from top to bottom: G-10 currencies, US stock indices, US Treasury rates, crude oil, precious metals, and grains and oilseeds.
[173] This hypothesis is not perhaps that unrealistic, as even DARPA (US Defense Advanced Research Projects Agency) is working on it as part of its "Financial Markets Vulnerabilities Project" (source: see bibliography [107]).
[174] See bibliography [108].

5. Cyber Dissemination of False Information

The dissemination of false information is an age-old stock market manipulation technique. One example is the false announcement of the death of Napoleon Bonaparte, a hoax orchestrated in February 1814 at the London Stock Exchange to increase in the price of British government bonds.[175] No one can dispute, especially with the current debates on "fake news"[176] and specific new laws,[177] that in the digital age, with websites, social media and email, the dissemination of false information has become much easier, faster and has a much broader scope. The impact on financial markets, buoyed by instant information[178] and rumours, is therefore much more significant. For example, on 27 June 2017,[179] a fake news item consisting of a simple photo of a helicopter crash with a few words about the death of Vitalik Buterin, the creator of Ethereum, was enough to cause this cryptocurrency to lose $4 billion in value in a single day. Similarly, on 22 November 2016, a false press release issued by Vinci alleging the discovery of accounting fraud drove the company's share price down by nearly 19% in seven minutes, representing a temporary loss of market capitalisation of around €7 billion.

The motivations for disseminating false information are often economic[180] (the criminal seeks to profit personally in economic terms from the transaction), but they can also be activist,[181] given the great symbolism and potentially significant impact on the valuation of the companies targeted. Undoubtedly, economic sabotage by a competitor or state destabilisation can also be considered as alternative motivations.

The dissemination of false information can, like cyber insider trading, affect all those involved in the information dissemination chain in the stock market world. Specialised financial information providers (such as Bloomberg or Reuters) are naturally often the first to be targeted. In the past, influential rating agencies have also been able to disseminate false information without any manipulation. There are many sources of financial "misinformation", and it is obvious that misinformation finds highly effective allies in social media, especially Twitter.

5.1. Cases

5.1.1. The Vinci Galaxy

[175] See bibliography [109].
[176] Latest article showing the extent of the phenomenon: see bibliography [110].
[177] See bibliography [111].
[178] Thanks to high-frequency algorithmic trading and the automated reading of financial news.
[179] See bibliography [112].
[180] There does not seem to be any fundamental difference between the motivations of attackers focused on stock market cybercrime and those of attackers focused on traditional cybercrime, where three quarters of attacks are motivated by economic profit (source: https://www.hackmageddon.com).
[181] This aspect will be revisited in the case analysis. An example of famous activists is the "Yes Men" in the United States. This is an environmental activist organisation specialising in the production of fake news that has targeted multinationals, particularly oil companies. In 2010, the US giant Chevron was the victim of a very sophisticated hoax, with a hijacked advertising campaign that made it seem that it was accepting responsibility for several environmental disasters. In 2011, it was the turn of the US industrial conglomerate GE, which was accused at the time of benefiting from undue tax favours. It was targeted by the Yes Men who used a false press release to announce that GE would return $3.2 billion to the tax authorities. The Yes Men had gone so far as to hold a fake press conference in Washington, posing as representatives of the Chamber of Commerce, until a real Chamber of Commerce member arrived and revealed the stunt.

Case: Emulex: "The Mother of All Hacks"[182]

Summary: On 24 August 2000, Emulex, a NASDAQ-listed company specialising in optical fibre, saw its share price fall from $113 to $43 in just eighteen minutes, representing a 60% drop in the company's value. This followed the publication of a false press release on Internet Wire (a financial information provider), reporting the resignation of its chairman, the opening of an investigation by the SEC and the downward revision of its turnover. This false press release was actually written by a 23-year-old student named Mark Jakob, who had worked at Internet Wire for the online stock market information service. A savvy connoisseur of internal processes, Jakob called the appropriate person to notify them of the imminent arrival of the press release and sent it by email to Internet Wire from an open access computer in the library of his former university. Since the correct protocol had been followed, Internet Wire did not bother to check the content of the press release. It was published on 24 August 2000, and very quickly picked up by several press services, such as Bloomberg and Dow Jones.[183] The reaction was immediate, the share price fell rapidly. Jakob then bought shares at the lowest possible price, on the internet from a hotel room in Las Vegas, allowing him to close the short position of 3,000 shares he had previously taken on 17 and 18 August 2000 and take a new long position of 3,500 shares which he closed at a profit on 28 August 2000, once the false information had been denied and the share price had risen. In parallel with the public relations activities to deny the false information, the company filed a complaint and brought in the FBI and the SEC. The investigation resulted in the arrest of the alleged offender on 31 August.

Profit: Temporary loss of market capitalisation of around $2.5 billion. The profit generated for the criminal, however, was only $241,000.

Case: Whitehaven Coal[184]

Summary: On 7 January 2013, a false press release apparently issued by ANZ Bank announced that it had cancelled a $1.2 billion loan to the Australian mining company Whitehaven Coal for the Maules Creek project, citing several economic and environmental reasons. The mining company's share price then fell by 9% to $3.21 in the space of a few moments before trading in its shares was suspended. An ecological activist group called "Front Line Action on Coal" claimed responsibility for the action. Lead instigator Jonathan Moylan (26 years old) pleaded guilty and was sentenced to 1 year and 8 months in prison but was released immediately subject to good behaviour and a fine of $1000.[185]

Profit/Impact: Temporary decrease in market capitalisation of $315 million. However, one press article estimates the "real" loss to shareholders at only $450,360[186] (see the discussion below, which generally estimates the real damage at between 1/1000 and 1/100 of the loss of market capitalisation).

[182] See bibliography [113].

[183] At the same time, a class action was brought by the retail investors affected against Internet Wire and Bloomberg, companies specialising in the distribution of financial press releases, claiming that these companies had unintentionally disseminated false information. The two companies were accused of failing to comply with internal controls by not verifying the accuracy and authenticity of the Emulex press release before it was published. According to the complaint, Internet Wire received the press release on the afternoon of 24 August, while the markets were not due to open until the morning of 25 August. During this critical period, the media outlets should have examined the information in greater depth. Finally, Emulex had historically used Business Wire magazine and not Internet Wire to distribute its press releases. This change in the distribution medium should therefore have led to greater care in reviewing the information communicated. Following this case, checking the authenticity of press releases issued by professionals should be improved.

[184] See bibliography [114].

[185] See bibliography [204].

[186] See bibliography [205].

Case: Fingerprint Cards[187]

Summary: On 11 October 2013, a false press release was issued announcing the acquisition of the Swedish company Fingerprint Cards, specialising in digital recognition, by Samsung for $650 million. This press release, although false, was even published on the official Fingerprint Cards website. The share price soared by nearly 50% in the space of ten minutes before trading was suspended. The facts were reported to the police and Sweden's stock market regulator. The outcome from the investigation is not known.

Profit/Impact: Temporary increase in market capitalisation of $200 million.

Case: G4S[188]

Summary: On 12 November 2014, G4S, a security company responsible in particular for the surveillance of migrant camps with a market capitalisation of £3.638 billion, was the victim of a false press release announcing an accounting audit and the dismissal of its CFO. The G4S share price was only slightly impacted (0.94% down initially, ending the day up 2%) by the distribution of this false press release because, even though it may have misled some journalists and caused many tweets, it was not picked up by Bloomberg. A demand by political activists for action against repressive anti-migrant policies was also issued after the false press release.

Profit/Impact: Temporary loss of more than £40 million in market capitalisation, but relatively insignificant compared to the volatility of the share price. No criminal profit, to our knowledge. It does not appear that an investigation has been initiated or successfully completed by the authorities.

Method: The fake email used a domain name that had been registered about a fortnight earlier under a fake Dutch identity and which closely resembled the official G4S address. Furthermore, the hoax seemed somewhat crude with spelling mistakes and missing words. More importantly, it was not picked up by the London Stock Exchange's Regulatory Information Service (RIS), which is supposed to be the central point for all official announcements of companies listed on it. More interestingly, in some demands relating to the G4S case on alternative media sites such as Indymedia, authors recommended using a guide called "Prank the pranksters! Playing around with information and fakes in the age of immaterial capitalism."[189]

Case: Immunovaccine[190]

Summary: On 3 March 2015, a false press release announced a major partnership between the Canadian pharmaceutical company Immunovaccine and Gilead Sciences. Immunovaccine's share price jumped by 24% and trading in its shares was then suspended.

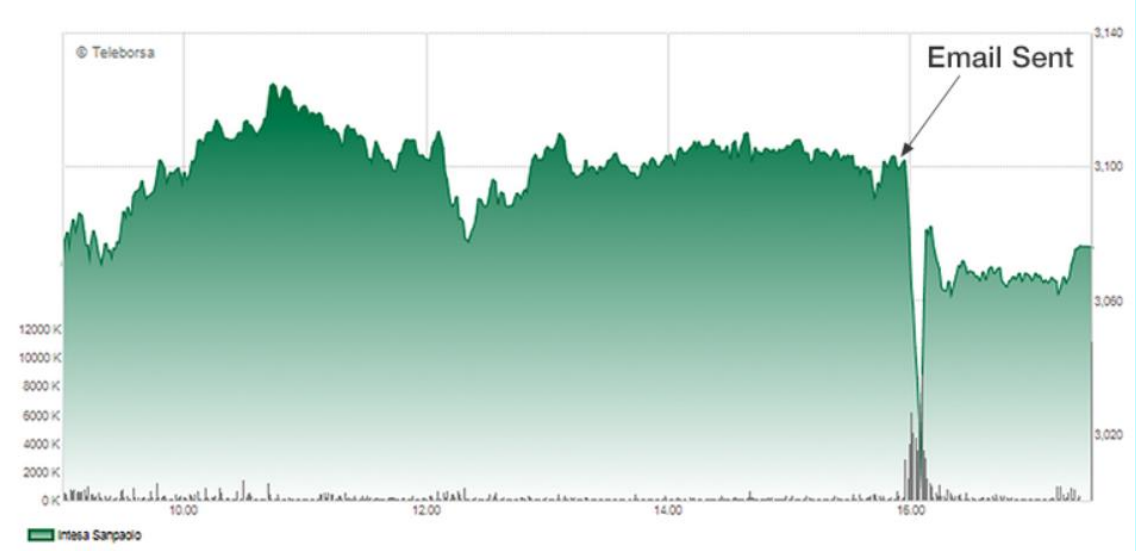
Profit/Impact: The Investment Industry Regulatory Organization of Canada (IIROC) announced that it would cancel transactions made during the hoax or change the price of transactions to their original value.

Case: Banca Intesa[191]

Summary: On 24 April 2015, Banca Intesa Sanpaolo, one of Italy's largest banks, was the victim of a false press release that announced accounting discrepancies with an impact of €2 billion on its results and the dismissal of its CEO, Carlo Messina. The share price was significantly impacted, suffering a sharp 4% drop in just eight minutes to €2.99 before rebounding rapidly to its previous level.[192] On an alternative media website called Indymedia Piemonte, the ecological activist group "No Tav" claimed responsibility for the

[187] See bibliography [206] and [207].
[188] See bibliography [115].
[189] See bibliography [116].
[190] See bibliography [208] and [209].
[191] See bibliography [117], [118] and [119].
[192] See the graph above where "Email Sent" refers to the initial sending of the false press release by email.

action. “No Tav” was fighting against the Lyon-Turin high-speed train project, to which Banca Intesa was a contributor.



Profit/Impact: Temporary decrease of €2 billion in market capitalisation. To our knowledge, the investigation is still ongoing.

Method: The fake email used an intesasanpaolo-group.com domain name that had been registered three weeks earlier under a fake Italian identity and which closely resembled the official address intesasanpaolo.com. The fake email referred to a mirror site that was identical in every respect to the official Banca Intesa site, except for the press release. Cybercriminals even took the trouble to reply to journalists’ emails, signing their replies with the name of the Group’s real media relations manager. The hoax was therefore not crude, and the modus operandi was very close to those used in the G4S and Vinci cases.

Case: Twitter Takeover[193]

Summary: On 14 July 2015, a fake article apparently from Bloomberg announced a takeover offer for Twitter of $31 billion (compared with the previous day’s valuation of $25 billion). The information contained in the article was then shared by a CNBC star presenter in a tweet.[194] The Twitter share price soared by 8% in ten minutes. It should also be noted that behind every rumour there may be an ounce of truth and that, in the case of Twitter, persistent rumours about its poor health and a possible takeover were already doing the rounds. Bloomberg’s quick denial was enough to restore the share price to its previous level in less than five minutes.

Profit/Impact: Market capitalisation increased by $2 billion. There was apparently no personal criminal profit. The investigation still appears to be ongoing.

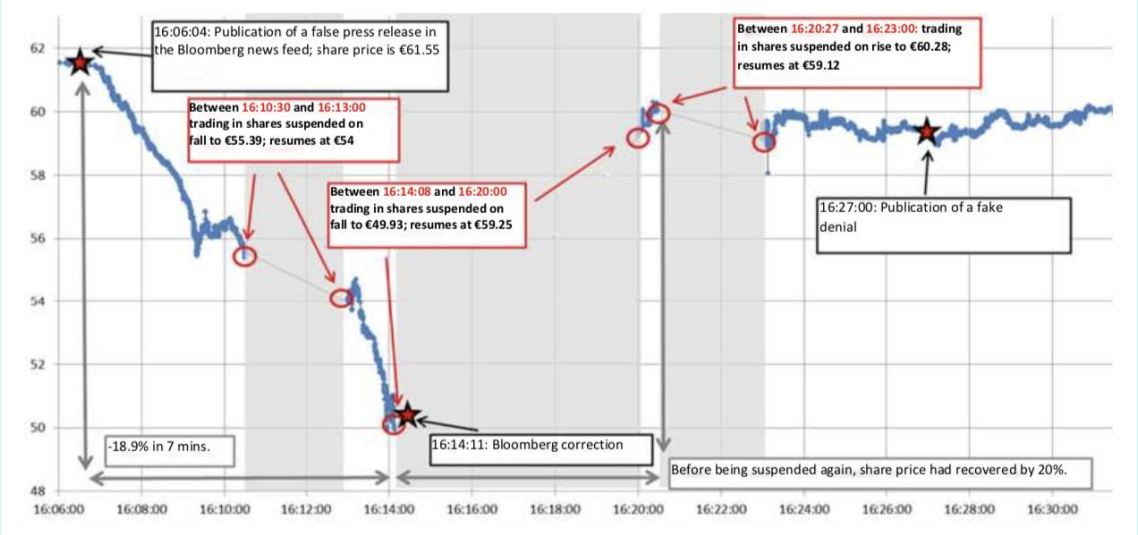
Method: A fake Bloomberg.market website, which was an identical copy of the real Bloomberg.com website, had been registered four days earlier. The name of the author on the fake article was that of a real Bloomberg journalist.

[193] See bibliography [120].

[194] This single tweet cannot really be implicated, and it is obvious that the webcrawlers had their role to play in spreading this news.

Case: VINCI[195]

Summary: On 22 November 2016, Vinci was the victim of a false official press release announcing the discovery of accounting errors amounting to €3.5 billion and the dismissal of the CFO responsible for these errors. More specifically, at 16:05, the false press release was sent by email to several specialised editorial offices. At 16:07, the information was distributed by the Bloomberg agency, with Vinci's share price falling by almost 19% in the space of seven minutes, equivalent to a loss of market capitalisation of €1 billion per minute. Bloomberg's denial at 16:14:11 allowed the share price to recover almost all its value as quickly as it had lost it. At 16:27, a fake denial by the criminals added to the confusion in some newsrooms but this did not cause significant impact on the already stabilised share price. Finally at 17:35, a further false statement making pseudo-activist[196] demands was sent by email.



Profit/Impact: Temporary decrease of more than €7 billion in market capitalisation. The losses made could be lower (see discussion below).

Method: The fake email used a vinci.group domain name that had been registered several days earlier under a fake Dutch identity and which closely resembled the official vinci.com domain. The fake email referred to a mirror site that was identical in every respect to the official Vinci site, except for the fake press release. The fake press release also stated the name of the real press relations officer but provided a fake phone number. A few calls made by journalist to this number were answered by the hoaxer. The hoax was therefore not a crude one. The modus operandi was very close to those used in the G4S and Banca Intesa cases.

Case: Fake Letter from the CEO of BlackRock[197]

Summary: On 16 January 2019, a few days before the official publication of the annual letter from the CEO of the famous US management company BlackRock, Larry Fink, a fake email was sent to several media outlets that spoofed his identity by using the email address "larry.fink@blackrock-esg.com" and referred to a fake website that was created to look like the official BlackRock website. This letter mentioned an environmental and ecological shift for BlackRock and disinvestment in companies that do not comply with the Paris agreements. On the same day, at 14:31, BlackRock refuted this information in a tweet on its

[195] See bibliography [121] and [122].
[196] Most of those involved its authenticity because of its style and content.
[197] See bibliography [210].

official account. No apparent impact on share prices was observed as a result of this misinformation that was clearly activist in nature.

It should be noted that, when confronted with this type of cybercrime, which requires few resources and can be easily carried out anonymously, investigators are often more likely to succeed if they follow the digital trail left by a cybercriminal's stock market transactions. There are many freely accessible resources on the internet that allow novice cybercriminals to perfect their skills when it comes to creating their stock market hoax.[198] It is also very easy for the fraudster to remain anonymous on the internet, either by using public Wi-Fi, VPN[199] or the TOR network,[200] especially since the identity checks required when registering a domain name or hosting a website are almost non-existent and the data retention period is short. Using payment methods such as prepaid cards or cryptocurrencies also makes it possible to pay for these services without breaking one's anonymity.[201] Since investigations often have an international scope, cooperation between the various national regulators is essential here. However, in practice, the widespread disparity in their powers to deal with often unregulated entities and the relative slowness of communication between them are powerful obstacles to the use of digital evidence. For cybercriminals, the investment and risks involved are therefore rather low, but the impact is potentially very significant, since it can amount to a *temporary* loss of market capitalisation of several hundred million or even billions of euros. The circuit breakers (or trading curbs) implemented at stock exchanges do, however, have the ability to stop too great a drop.

In *"Les 3F du HoaxCrash : Fausse donnée, Flash Crash et Forts profits"* ("The 3 Fs of HoaxCrash: False Data, Flash Crash and Formidable Profits"), the authors, after presenting in detail the 2016 Vinci case and briefly other similar cases, define three interesting parameters: the validity period of a hoax before publication of a denial; the effectiveness of the hoax, defined as the ratio of the gains realised by the attacker to the (Kolmogorov[202]) complexity of the modus operandi; and the power of the hoax, defined as the ratio of the total price variation to this same complexity. Finally, in view of the speed of events, they propose, without specifying its exact nature, developing a network of intelligent agents that evaluate in real time the veracity of published messages in order to avoid new cases.

Defining the power of a hoax is essential, since manipulation will often cause the share price to change significantly and abruptly without the criminal being able to take full advantage of it (or wanting to take advantage of it in the case of an activist). This concept could be refined by weighting this power, firstly, by the usual volatility of the share price (because changing the price by x% for a very volatile share price

[198] At least one document – prankthepranksterpdf – is available online. This truly is a manifesto and bible that details everyone involved in an operation as well as all the steps and tips to carry out a successful stock market hoax. It explains why and how to prepare and distribute a fake financial press release, obtain journalists' email addresses, create fake websites, send fake emails using the weaknesses of the SMTP protocol with Telnet while ensuring the hoaxer remains anonymous, etc.

[199] VPN stands for "Virtual Private Network". A "virtual" private network allows a direct, secure connection to be created between two remote computers. Companies therefore provide VPN services by establishing a VPN between your computer and their server. When connecting to the internet on your computer, only the IP address of this server is visible. Of course, companies offering VPN-type services may or may not register your connections and therefore your original IP address.

[200] TOR stands for "The Onion Router". It is a global, decentralised computer network whose servers are also called nodes. This network can anonymise the origin of internet connections (the often mentioned original IP address) by bouncing traffic between different nodes, which only know the IP address of the previous and next node. TOR also provides its users with a range of hidden services, by hiding the identity of the server that hosts them. This server will receive an address ending in .onion and will only be accessible by using TOR. TOR is part of the notorious Dark Web.

[201] Even though some payments made in bitcoins can be tracked, it appears that not all Bitcoin/FIAT exchange platforms are demanding in terms of "Know Your Customer" (KYC). European legislation is changing in this respect, but global harmonisation is still a long way off.

[202] The Kolmogorov complexity, in information theory (or random complexity or algorithmic complexity), of an object (number, digital image, string) is the size of the smallest algorithm (in a certain fixed programming language) that generates that object. This quantity can be seen as an evaluation of a form of complexity of the object. Source: Wikipedia.

is not the same as changing a price by x% for a very stable share price), and secondly, by the prices and volumes of transactions actually made on the market during the validity period of the hoax (because a single share traded at the lowest price is not the same as a million shares traded, in terms of both the "reliability" of the share price and the potential victims who sold; and this is especially true in the case of a hoax, where the value quickly returns to its original level).

A quick analysis of the orders of magnitude would tend to prove that the loss actually incurred by shareholders trading during the hoax period would be 100 to 1000 times lower than the "naive" loss of market capitalisation.[203] We will not dwell on this subject and will only consider, in the analysis of our cases, the gains realised by the criminal and the almost instantaneous change in market capitalisation, which, although open to criticism for the reasons mentioned above, remains an evocative, simple and robust indicator.

Finally, it is clear from all these cases, which have an almost identical modus operandi, that the question of the dissemination of "official" financial information is crucial. These cases show the need to work together with all the parties concerned (listed companies, information distributors, stock market regulators,[204] stock exchanges,[205] etc.) to consider measures to prevent such incidents from occurring or to limit their consequences. Following this incident, for example, in its press release of 23 February 2017,[206] the AMF defined a number of best practices for issuers and news agencies, aimed, firstly, at clarifying the official channel for disseminating information about the issuer to better ensure its authenticity and, secondly, at strengthening the awareness and cybersecurity procedures at news agencies to avoid any hoax upstream (receiving a false press release considered to be true by journalists in the above cases) or downstream (dissemination of a false press release directly into the news agency's or information provider's information systems).

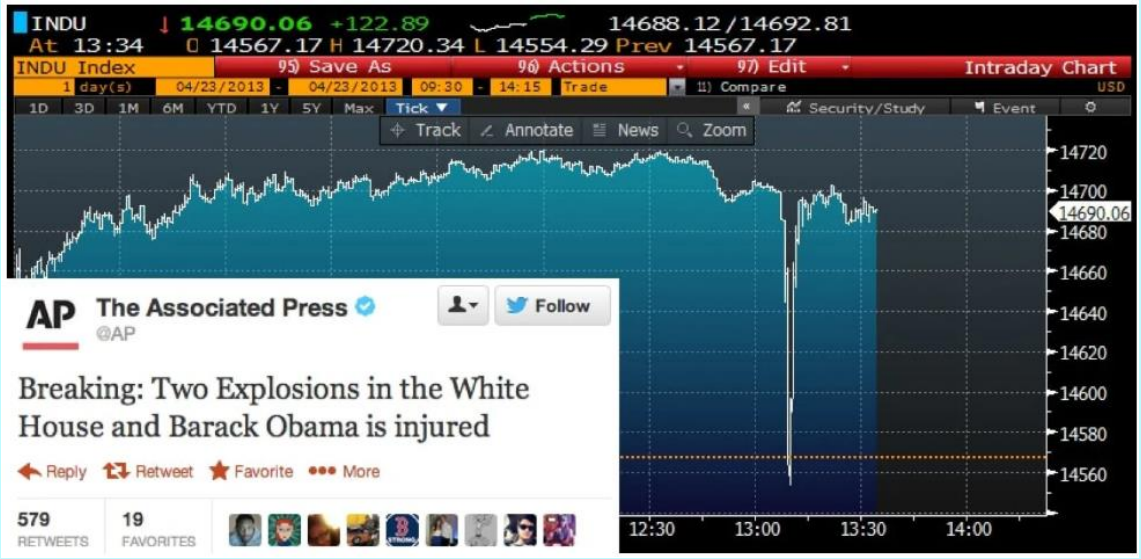
5.1.2. Dissemination of False Information by Twitter

Case: AP's Obama Tweet[207]

Summary: On 23 April 2013, the Associated Press (AP) Twitter account, followed by two million people, was compromised and hacked, and at 13:08 the following message was sent: *"Breaking: Two Explosions in the White House and Barack Obama is injured."* The share prices of many financial instruments instantly

[203] In this respect, the Vinci case is both illuminating and symbolic. The 19% decrease (in less than 10 minutes) corresponds to €7 billion in market capitalisation. However, if we look only at the transactions carried out during the period of decline (just over one million shares sold at prices varying between €61.50 and €50), the approximate loss suffered by the victims, who would therefore have sold their Vinci shares at a price (approximately €55.75, the average between €61.50 and €50) that was lower than the "pre-false announcement" price of €61.50, would only amount to around €6 million.
In general, and focusing on obtaining orders of magnitude only, a hoax resulting in a x% drop in the share price in 10 minutes will result in a "naive" reduction in market capitalisation of x%, but in reality will have a maximum detrimental impact (MDI) on market participants (not including the consequences to their reputation or image) of only MDI=(x% price/2)(10/480)(panicvolumefactor)(Ndaily) where (x% price/2) represents the loss of earnings per share in euros, (10/480)(Ndaily) represents the average quantity of shares traded in 10 minutes, with Ndaily the daily volume traded, and panicvolumefactor represents the volume multiplier effect due to the news/panic.
If we replace the share price by TotMarCap/Ntot, where TotMarCap is the company's total market capitalisation and Ntot is the company's total number of shares, and by approximating (10/480)/2 with 1/100, we still have MDI=(panicvolumefactor)x% (1/100)(TotMarCap)(Ndaily/Ntot) or by estimating that the average volume of shares traded daily (Ndaily) represents about 1% of the total number of shares, MDI=x% (TotMarCap)(panicvolumefactor)(1/10,000), i.e. almost 100 to 1000 times (depending on whether one takes a panicvolumefactor of 100 or 10) less than the naive estimate of the change in market capitalisation.
[204] See the cases below relating to the dissemination of false information by the EDGAR regulatory reporting system.
[205] As seen in the G4S case, some stock exchanges also have an official central register for regulatory filings or announcements from issuers.
[206] See bibliography [123].
[207] See bibliography [124] and [125].

dropped by one percent, causing chaos in the markets. Denials from AP and the White House immediately restored calm, with share prices returning to their previous values within two minutes.



Profit/Impact: Almost instantaneous loss of market capitalisation, based on the S&P500, of $136.5 billion! The Syrian Electronic Army claimed responsibility for the attack, but investigations by the FBI and SEC still appear to be ongoing.

Case: Dissemination of Fake Tweets[208]

Summary: On 29 January 2013, a Scottish trader named Craig sent a series of eight tweets over a 90-minute period in which he wrote that Audience, Inc. was being investigated by the Department of Justice. He sent the tweets from an account registered by him but impersonating the identity and using the logo of the highly respected securities research firm called "Muddy Waters". Audience's share price plunged by 28%, resulting in trading in its shares being suspended. Trading resumed at previous levels once the hoax was revealed, notably by the "real" Muddy Waters. The next day, Craig repeated the process with another pharmaceutical company Sarepta Therapeutics, claiming that it was under investigation by the Food and Drug Administration (FDA), using a second Twitter account designed to impersonate that of Citron Research, another securities research firm. Since similar causes have similar effects, Sarepta's share price plummeted by 16%.

Profit/Impact: Around $100 for the cybercriminal (the low profit seems to be explained by the inappropriate timing of transactions). Nevertheless, there were (temporary) losses of market capitalisation for both companies of around $80 million for Audience and over $300 million for Sarepta.

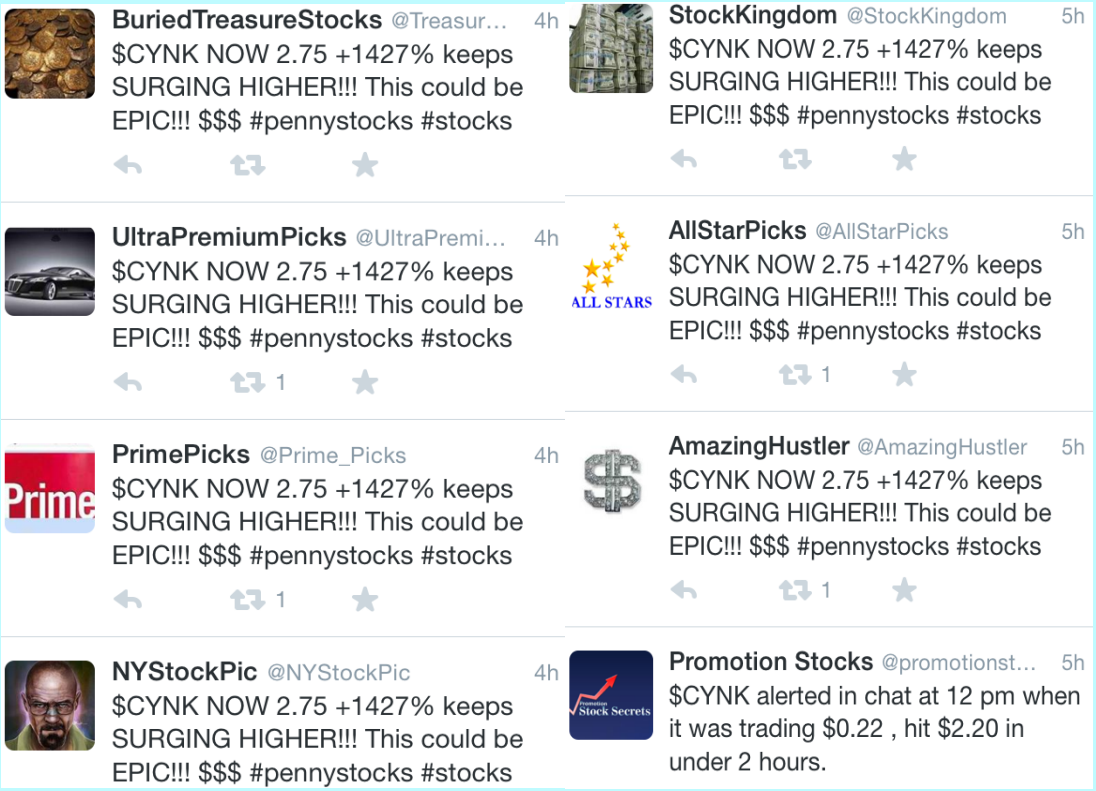
Case: CYNK[209]

Summary: This case is one of the most iconic pump-and-dump cases. A company, with assets worth no more than $1,400 and which had never previously been listed, had seen, in the space of a month (from 17 June to 10 July 2014), its share price explode to nearly $22 per share, for a market capitalisation of almost $4.5 billion. On 11 July, trading in its shares was suspended by the SEC. When trading resumed on 28 July, it shares traded at only $0.60 per share. The criminal, in this case the founder of the company hiding behind nominees, was charged by the SEC in 2015.

[208] See bibliography [126].
[209] See bibliography [127], [128] and [129].

Profit/Impact: The SEC halted trading in the company's shares before the criminal could make a profit from selling the shares he controlled. However, retail investors did lose out. Increase in market capitalisation of almost $4.5 billion.

Method: An intense promotional campaign using specialised websites and social media was used to attract new investor-victims.



Twitter, like all social media, is the ideal playground for spreading false information: almost anonymous, fast and able to reach a wide audience, thanks in particular to fake accounts that are sometimes automated (using "bots") and can be rented out at will. In 2018,[210] Facebook deleted more than a quarter of its accounts because they were allegedly fake, and in 2017,[211] a study revealed that at least 15% of Twitter accounts could be bots. All social media-type applications are affected, and WhatsApp deletes two million accounts per month in an attempt to combat false information.[212]

These "social bots" seem so capable of influencing people's opinion that DARPA (US Defense Advanced Research Projects Agency) became so concerned about them that held a competition[213] in 2015 specifically to identify these robotic influencers. Since then, the last US presidential election, with possible Russian interference through the use of these social bots, has confirmed DARPA's concerns, and interest in the subject has grown.[214]

We will not describe in detail the mechanisms at work in the dissemination of misinformation via social media, even though some results relating to the higher rate of spreading "false" information over "true" information may be perplexing.[215] It should nevertheless be pointed out that these techniques for

[210] See bibliography [130].
[211] See bibliography [131].
[212] See bibliography [211].
[213] See bibliography [132].
[214] See bibliography [215].
[215] See bibliography [133].

disseminating false information obviously work in favour of stock market cybercriminals, as in the cases described above (which are certainly not isolated cases), since the SEC has issued specific alerts[216] to warn retail investors against rumours and recommendations that originate from social media sources and may be used for "pump-and-dump" manipulations. For example, in his article "Market Manipulation and Suspicious Stock Recommendations on Social Media",[217] Thomas Renault shows, by analysing several million messages sent on Twitter relating to small capitalisation shares, that abnormal activity is often associated with a large increase in share price on the event day and a decline the following week. In addition, this abnormal activity seems to be concentrated in certain clusters of Twitter accounts, supporting the manipulative campaigns hypothesis. While the examples so far have been limited to equities, it should be noted that the entire financial sector may be affected.

Finally, it is important to remember that automation coupled with the need for speed at all costs, the natural propensity of financial players to be informed of rumours[218] and the existence of specific algorithms whose trade orders are directly linked to the content circulating on social media, whether simply through the automated reading (without human intervention) of the content of Twitter accounts from official sources or through more complex signals based on the analysis of Twitter's own activity (analysis of feelings, hashtags or behaviour, etc.), makes financial markets even more likely to succumb to this type of manipulation.

5.1.3. Dissemination of False Information by EDGAR

Case: EDGAR IDTI[219]
Summary: On 12 April 2016, Aly, a resident of Pakistan, acquired a large block of out-of-the-money call options with a very short expiration date in Integrated Device Technology, Inc. ("IDTI") shares. A few minutes later, Aly filed a false filing (Schedule 13D) on the US stock market regulator's EDGAR website, in which he stated that he and a group of other people had acquired more than a five percent beneficial interest in IDTI and had made an offer to IDTI's board of directors to buy the company at a 65% premium to the market price. Following this false filing, which was made instantly public by EDGAR, IDTI's share price soared by 25% in less than 10 minutes, and Aly was able to sell his options at a profit. Thirty minutes later, Aly cancelled his regulatory filing on EDGAR.
Profit: A profit of $425,000 for Aly. An increase in the company's valuation of $750 million.
Method: False filing on the stock market regulator's official website.

Case: EDGAR FITBIT[220]
Summary: On 10 November 2016, Robert W. Murray purchased call options in FITBIT shares a few moments before filing on the EDGAR website a fake tender offer (Schedule TO-C) for this company at a premium of almost 50% above the market price. The share price rose 10% in 10 minutes, and Murray seized the opportunity to sell his options at a profit only 15 minutes after his false filing.
Profit: $3,100 for the criminal, but an increase in the company's market capitalisation of $913 million.
Method: Murray created a fake email account by fraudulently using the name of a senior manager randomly selected from the internet to register on EDGAR. He then declared that this person was the CFO

[216] See bibliography [134].
[217] See bibliography [13].
[218] One of the selfish solutions to limit the possible damage caused by misinformation on the markets is always to be the first. After all, it does not matter if the information is true or false; what matters is knowing what effect this information will have on the market! As the old saying goes: "Better to be wrong with the market than right all alone."
[219] See bibliography [135].
[220] See bibliography [136].

of a fake company (ABM Capital) that was responsible for the tender offer, by forging the signature of a notary. After researching several previous cases pursued by the SEC and recognising the importance of IP addresses in the SEC's investigations, Murray tried to hide his true identity by using a proxy for his IP address. Unfortunately for him, Murray bought his options using an IP address registered in his employer's name.

Case: EDGAR AVON[221]
Summary: On 14 May 2015, a Bulgarian trader named Nedko Nedev filed a false tender offer for the AVON group from a false entity called PTG Capital Partners Ltd. at a premium of 181% (above the previous day's closing price) in the EDGAR regulatory system after taking a position on the AVON shares using a CFD.[222] Once the false information was released, the share price soared by 20% in 20 minutes, from $6.60 to $8. The volume of trade also exploded by 448%. On 13 December 2012, the same modus operandi was used on Rocky Mountain shares, with an impact of 4.6% on the share price and 1,780% on volume of trade, and also on 13 May 2015, on Tower Group shares, with an impact of 32% on the share price and 1,963%.
Profit: Only $5,000 of personal criminal profit, but an increase in AVON's market capitalisation of almost $600 million.

5.2. Perspectives

5.2.1. Very Wide Scope

While the cases presented above are limited to the dissemination of false information relating to a particular issuer (except in the AP Tweet case, which had a systemic effect) and the impact on its share price, no doubt because the stock market is the largest public market, it is important to remember that the stock market world is much broader and that there are very many opportunities. For each asset class (equities, credit, interest rates, exchange rates, commodities, energy, real estate, etc.), there is a wide range of financial instruments, the price of which varies according to several pieces of data.

Take for example the factors influencing the price[223] of a rather confidential sub-family of raw materials such as livestock,[224] including diseases affecting livestock, extreme weather conditions in producer countries, consumption patterns and purchasing power in consumer countries. It is easy to imagine false information for each of these factors and, with that information, provided that the most effective way to disseminate it is found (each market having its own particular practices and sources of information), manipulating the price of livestock futures.

The "credit" asset class, as far as companies and sovereign issuers are concerned, is strongly influenced by the ratings issued by rating agencies. For example, on 10 November 2011,[225] Standard & Poor's, in an email sent to some of its subscribers, mistakenly stated that the French sovereign debt rating had been downgraded. The announcement, which came at a time when France's AAA rating was clearly in jeopardy, sent stock markets reeling at the height of the eurozone's debt crisis. The rating agency later issued a statement claiming that the error was caused by a technical problem in its computer system. Based on

[221] See bibliography [137].
[222] A CFD (Contract for Difference) is a derivative product that allows identical exposure to changes in the share price multiplied by a pre-determined leverage effect.
[223] See bibliography [138].
[224] Livestock futures are traded on the Chicago Mercantile Exchange (CME).
[225] See bibliography [139].

this and other highly informative cases of errors by rating agencies,[226] it is easy to imagine how they could also be the target of cyber insider trading by stealing ratings or of the cyber dissemination of false information by impersonating these agencies or by directly modifying the data used to calculate ratings or the ratings themselves in their systems.

The possibilities are therefore endless and would benefit from being mapped out in detail.

5.2.2. Fake Data

The previous cases involved false information fabricated from scratch as false financial press releases, which is closer to creating a traditional fake story ("fake news") than to fake data. However, in a world that is becoming increasingly dependent on data every day, which is especially true in the stock market world, how could we ignore the fact that that this financial data, such as the sensitive economic indices and indicators used for cyber insider trading described above, could not only be stolen, but also modified or corrupted?

A recent report by Accenture[227] shows how data integrity is a critical risk factor for financial institutions. For example, according to a survey of 800 companies, more than half of them do not have a robust system in place to validate and ensure the quality of their data, while most of them recognise that there is an increasing use of this data to automate investment decisions, leading to a high risk of manipulation.

If, as seen above, it is sometimes possible to mislead journalists employed by major financial information providers such as Bloomberg or Reuters into unwittingly disseminating false information, one may well ask whether it is also possible to penetrate these companies' computer networks to modify further downstream the market data disseminated to the entire financial community over Bloomberg terminals or through Reuters professional applications. Given the presence of these two companies on the financial markets (more than 50% market share between them) and the credibility they bring to the information they disseminate, their cybersecurity measures and the ways in which their data is delivered to customers remains a key issue, which, for the moment, does not seem to have received the attention it deserves.

5.2.3. Deepfake and Artificial Intelligence

The rapid emergence of artificial intelligence or, at the very least, of sophisticated learning techniques or machine learning, also opens up new opportunities for the cyber dissemination of false information. The opportunity afforded by the many easily accessible tutorials on the internet[228] to falsify videos by "making anyone say anything in any way" (known as "deepfake") makes false information even more credible and therefore its dissemination even more effective.[229] Governments, and particularly the US government, are already seriously concerned about the potential for misinformation from this new threat in the context of elections.[230]

[226] See bibliography [140].
[227] See bibliography [141].
[228] See bibliography [142], [143], [144] and [145].
[229] See bibliography [146] and [147].
[230] See bibliography [212] and [213].

Even if today's videos do not yet look and sound perfect,[231] how long will it be before a rumour circulates on social media with a supposedly hidden video from the Governor of the FED or the ECB discussing in private a hike in interest rates or a video showing a well-known activist fund revealing their next target?

Finally, the emergence of "intelligent" robots, capable of recreating human behaviour in a realistic way under certain conditions, will make it even more difficult to detect "social bots" and therefore the dissemination of false information as well. Similarly, the ever-increasing presence of robot advisors in the relationship between individuals and financial service providers also raises questions about their cybersecurity, which, once compromised, could be a vehicle for disseminating false information or false investment recommendations on financial instruments.

[231] See bibliography [148].

6. Cyberattacks on Stock Exchanges

When we talk about stock market cybercrime, we instinctively think of cyberattacks on stock markets themselves. Even though the AMF would not necessarily be the competent investigative authority,[232] it would be difficult to exclude the subject, since the stock exchange is, by its very nature, the heart of the system.

In a 2013 survey[233] of 46 stock exchanges, the International Securities Commission Association (IOSCO) reported that more than half had already suffered a cyberattack that year. The most common cyberattacks were those that used malware, denial of service (DoS) or distributed denial of service (DDoS) attacks. Ultimately, the cyberattacks suffered were considered to have had no effect on the proper functioning of the market and resulted in only minimal costs (less than $1 million) for the stock market. As an example, in 2012, a wave of DDoS attacks led by activists[234] hit the NYSE, NASDAQ and BATS stock exchanges in the US, but trading systems were not affected.[235] While there are no recent cases of DDoS attacks against a stock exchange,[236] DDoS attacks on the financial sector are still effective, despite the high costs incurred by this sector. For example, on 27 and 28 January 2018,[237] DDoS attacks by a single teenager slowed down or even crashed ABN Amro's online and mobile banking services, along with those of its ING and Rabobank sister banks. Several old cases are nevertheless interesting to note.

Case: Hong Kong Stock Exchange 2011[238]
Target: Stock Market
Summary: In 2011, an attack, apparently of Chinese origin, caused trading in the shares of seven companies to be suspended and even the temporary closure of the Hong Kong stock exchange. The attack reportedly compromised this stock exchange's official regulatory information dissemination website, preventing these seven companies from reporting their results through the usual channels and forcing them to find alternative valid means of reporting.

Case: Warsaw Stock Exchange 2014[239]
Target: Stock Market
Summary: In November 2014, the Warsaw Stock Exchange was reportedly compromised by a cyberattack by ISIS jihadists, who claimed responsibility and were able to steal a considerable amount of confidential information such as emails and diagrams of the internal computer network. Following this attack, cybercriminals exposed 41 stock broker logins and passwords to access the trading system. The attack apparently had no impact on the proper functioning of the market, but it illustrates how the exchange's trading accounts could be hacked.

[232] Depending on the nature and effect of the attack, it may or may not be characterised as "market manipulation". Moreover, as a market operator with the potential to have a systemic impact on the financial sector, the stock exchange is often the focus of several regulators, probably including the ANSSI, ACPR and AMF.
[233] See bibliography [149].
[234] See bibliography [150].
[235] If trading systems (the "core engine" or "matching engine") are compromised by cybercriminals, it is easy to imagine them taking advantage of this compromise by "artificially" increasing or decreasing the price of their respective sell or buy position.
[236] Except for the recent cyberattack on the Hong Kong stock exchange on 6 September 2019. See bibliography [221].
[237] See bibliography [151].
[238] See bibliography [150] and [152].
[239] See bibliography [153].

Case: "NASDAQ is owned", NASDAQ 2012[240]

Target: Stock Market

Summary: From May 2007 to 2011, Russian hackers successfully compromised NASDAQ's internal IT network. The cybercriminals first used SQL injections on the NASDAQ site to obtain access and then installed malware to obtain persistent access (a backdoor). They did not steal any particular information except for administrator logins and passwords. One of the hackers reportedly wrote to one of his accomplices: "NASDAQ is owned." Trading systems were apparently not affected by the attack, which focused specifically on the corporate network.

[240] See bibliography [154], [155] and [156].

7. Stock Market Cybercrime and its Aggravating and Mitigating Factors

8. Conclusion

For several years, and the subject has often been referred to in the press, cybercrime has been invading our world and now poses a major threat. The in-depth analysis of a methodology for estimating its cost, known as the market methodology and based on the average impact of a cyberattack on the share price of the victim company, which various studies estimate to range from -1% to -5%, shows that the uncertainties around quantifying it are extremely high. Nevertheless, an estimate of 0.5% of world GDP may seem reasonable. In any case, cybercrime is already (or is fast becoming) the most expensive form of crime, and it already accounts for almost 10% of the internet's overall economic contribution. The financial sector, and more particularly the stock market sector, are not immune to this cybercrime. However, it does seem more difficult to associate them with a specific cost unless a new and more in-depth study is carried out.

By explicitly excluding any cybercrime linked to cryptocurrencies, which also deserves its own specific study, stock market cybercrime is structured around the following three regulatory breaches: cyber insider trading (e.g. hacking to obtain inside information); cyber dissemination of false financial information (e.g. creating "fake" websites or fake rumours on social media influencing the share price of a listed company); and cyber price manipulation (e.g. hacking into trading accounts to set up a pump-and-dump type scheme).

The analysis of real cases of cyber insider trading revealed that the entire chain of financial market participants (issuers, banks, lawyers, information distributors, stock market regulators, stock exchanges, etc.) could be affected, particularly as a result of attacks often based on a targeted phishing campaign, infected attachments or unauthorised access by IT employees. Some of these campaigns appear to have been orchestrated by highly specialised organised criminal groups. The monetisation of inside information or the means of accessing it on the Dark Web remains an issue that needs to be resolved, but it is certain that the massive data leaks of recent years will play a part in future cyber insider trading. Finally, the proliferation of entry points resulting from the growth in digital mobility, the Cloud and the IoT, and the sheer scope of inside information (e.g. indicators, indices, economic data on all asset classes) the production and dissemination of which is not necessarily very secure, will undoubtedly make cyber insider trading even more attractive and could be mapped out in more detail.

The cases of cyber price manipulation highlighted mainly stem from intrusion into retail trading accounts, where the cybercriminal, once in control of the compromised account, generally implements a rapid manipulative strategy of the pump-and-dump type. Nevertheless, there is at least one case of intrusion into a professional trading account by an organised group that specialises in financial cybercrime. Most trading applications, whether mobile or desktop, could have serious gaps in their security. Finally, since algorithms are at the heart of financial exchanges, compromising them, or the route by which their orders are transmitted to the stock exchange, for manipulative purposes seems to be a credible future strategy.

The cyber dissemination of false information, like cyber insider trading, can affect several market participants along the financial distribution chain. However, the initial targets are mainly specialised financial information providers such as Bloomberg or Reuters, or even sometimes the applications used by stock market regulators that receive submissions of certain mandatory filings from listed companies. When a cyberattack of this kind, often unsophisticated and with motivations that are mainly activist, succeeds, the changes in market capitalisation generated in just a few minutes are often in the order of several hundred million or even several billion euros, even when the stock market circuit-breakers limit them. By contrast, the risk for cybercriminals is very low, as they can easily remain anonymous. This is

why it is essential to strengthen the awareness and security procedures of information providers to avoid any hacking upstream or downstream (directly in their systems). An in-depth study of the current level of cybersecurity at Bloomberg or Reuters and the potential vulnerabilities would be extremely useful. Several cases also used the dissemination power of social networks such as Twitter for economic (promotional campaigns such as pump-and-dump) or activist purposes. The automation and speed of markets, boosted by algorithms, used especially for reading news feeds directly, make misinformation even more effective. The advent of artificial intelligence, with its numerous opportunities such as "deepfake" and intelligent "social bots", will make it even more difficult to detect false information, especially since financial markets have many asset classes potentially as yet unexplored by cybercriminals. Lastly, it should be kept in mind that sensitive economic data and other indicators can be not only stolen (as in cyber insider trading), but also modified for the purpose of disseminating false information!

Finally, cases in which the stock exchange itself is compromised do exist and attest to the reality of the threat. However, these cases are dated and limited to compromising the internal corporate network, with no impact on trading systems.

This report has shown the extent of stock market cybercrime, which affects or can affect the entire chain of financial market participants with extremely significant consequences over very short time scales. The existence of aggravating factors (technological developments, behavioural changes, structural characteristics of the stock market world and cybercrime opportunities) makes stock market cybercrime even more attractive. This is particularly true in a context where, despite widespread awareness of cyber risk and new laws on cybersecurity, personal data protection and "fake news", international cooperation continues to be difficult and the international legal framework is still ill-suited. Raising awareness and mobilising the various international regulators, such as the SEC (which created its "cyber unit" back in July 2017) and the AMF, therefore appears crucial if the rise in stock market cybercrime is to be curbed.

In its July 2017 risk mapping, the AMF highlighted the importance of cyber risks by focusing specifically on the subject, and subsequently, in its 2018-2022 strategic plan, it drew attention to how important the issue of cybercrime had become and its desire to develop new expertise to respond to it. In 2019, it announced short, thematic inspections on the cybersecurity measures implemented at management companies, with cybersecurity also being included in traditional inspections. Finally, the AMF regularly participates, generally with the Banque de France and the Treasury Department, in numerous international working groups focused on financial cybersecurity, such as the G7's Cyber Expert Group and the ESRB's European Systemic Group, or ad hoc groups of the Financial Stability Board (FSB) or IOSCO (the International Organization of Securities Commissions), and in the feedback campaigns run by ESMA, the AMF's counterpart at the European level, on the possible improvement of EU texts related to financial cybersecurity. At the European level, we also note the significant involvement of the European Central Bank (ECB) with the publication in May 2018 of the TIBER-EU penetration test framework[241] and in December 2018 of its expectations in terms of cyber resilience for market infrastructures.[242]

As this report was based solely on public data, either cases posted online by (mainly US) judicial authorities or articles in the specialised press on the internet, the overview is certainly not exhaustive, especially since many cybercrimes remain undetected or are detected later on.[243] Finally, since the time taken to

[241] See bibliography [219].
[242] See bibliography [220].
[243] We are of course referring to APT (Advanced Persistent Threat) attacks which are assumed to give priority to persistence in systems and therefore also to the ability to remove their traces.

investigate is considerable, the cases presented here are somewhat dated and therefore do not necessarily reflect the current state of stock market cybercrime.

Bibliography and References

1. WORLD ECONOMIC FORUM, *The Global Risks Report 2018 (13th Edition)*. 2018. http://www3.weforum.org/docs/WEF_GRR18_Report.pdf
2. GROUPE DE TRAVAIL INTERMINISTERIEL SUR LA LUTTE CONTRE LA CYBERCRIMINALITE, *Protéger les internautes (rapport sur la cybercriminalité)*. Février 2014. http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf
3. BOOS, R. La lutte contre la cybercriminalité au regard de l'action des Etats. Droit. Université de Lorraine, 2016. https://tel.archives-ouvertes.fr/tel-01470150/document
4. GORDON, M.S., *Statement before the House Financial Services Committee*, 14 septembre 2011 https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector
5. NETTITUDE, *Threat Advisory SWIFT Banking*, décembre 2016. https://www.nettitude.com/wp-content/uploads/2016/12/Nettitude-SWIFT-Threat-Advisory-Report-client.pdf
6. MWR INFOSECURITY, *Threat Analysis SWIFT Systems and the SWIFT Customer Security Program* https://www.mwrinfosecurity.com/assets/swift-whitepaper/mwr-swift-payment-systems-v2.pdf
7. AMF, *Cartographie des risques 2017*, 3 juillet 2017 https://www.amf-france.org/Publications/Lettres-et-cahiers/Risques-et-tendances/Archives?docId=workspace%3A%2F%2FSpacesStore%2F50b71ad3-51f9-403e-b884-c92ac8b4b040
8. AMF, *#Supervision2022 : l'AMF présente sa stratégie 2018-2022*, 18 janvier 2018 https://www.amf-france.org/Reglementation/Dossiers-thematiques/l-AMF/Plan-strategique-de-l-AMF/strategies-2018-2022-de-l-autorite-des-marches-financiers
9. https://www.sec.gov/spotlight/cybersecurity-enforcement-actions et https://www.sec.gov/news/press-release/2017-176
10. BERTHIER, T. *Les 3F du HoaxCrash : Fausse donnée, FlashCrash et Forts profits*, Janvier 2017 https://www.chaire-cyber.fr/IMG/pdf/article_hoaxcrash_revise_-_t_berthier_-_chaire_saint-cyr.pdf
11. PELIKS,G. *La cybercriminalité*, Mai 2013 https://www.forumatena.org/files/livresblancs/LaCybercriminalite.pdf
12. LIN, T.C.W. *The New Market Manipulation*, Emory Law Journal. http://law.emory.edu/elj/content/volume-66/issue-6/articles/the-new-market-manipulation.html
13. RENAULT, T. *Market Manipulation and suspicious stock recommendations on Social Media*, 31 Jul 2017 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3010850
14. NASSON,L et SMITH T.N et ZEYTOONIAN, A. *The future of financial crime and enforcement is cyber-based,* K&L Gates*,* 3 janvier 2018 http://www.klgates.com/the-future-of-financial-crime-and-enforcement-is-cyber-based-01-03-2018/
15. MINISTERE DE L'INTERIEUR, *Etat de la menace liée au numérique en 2018*, 20 juin 2018. https://www.interieur.gouv.fr/Le-ministre/Communiques/Etat-de-la-menace-liee-au-numerique-en-2018
16. US GOVERNMENT ACCOUNTABILITY OFFICE, *Costs of crime: experts report challenges estimating costs and suggest improvement to better inform policy decision*, septembre 2017 https://www.gao.gov/assets/690/687353.pdf
17. THE COUNCIL OF ECONOMIC ADVISERS, *The cost of malicious cyber activity to the US Economy*, Février 2018 https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf
18. SCOTT, P. *How much of a problem is cyber-crime in the UK*, 1 novembre 2016 https://www.telegraph.co.uk/news/2016/11/01/how-much-of-a-problem-is-cyber-crime-in-the-uk/
19. https://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud

20. EDWARDS, *E. DPC receives over 1100 reports of data breaches since start of PIBR rules*, 30 juillet 2018 https://www.irishtimes.com/business/technology/dpc-receives-over-1-100-reports-of-data-breaches-since-start-of-PIBr-rules-1.3580240
21. FIREEYE, *special report M-Trends 2018* https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf
22. PWC, *Managing cyber risks in an interconnected world*, 30 septembre 2014 https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf
23. KOPPE et KAFFENBERGER, L et WILSON Christopher. *Cyber risk, market failures and financial stability*, IMF Working Paper, 7 aout 2017. https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104
24. MCAFEE (CSIS), *Economic impact of cybercrime*, fevrier 2018 https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf
25. https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-comparison-france-en.pdf
26. RIOUX, P. La cybercriminalité coute 3,36 milliards d'euros aux entreprises françaises, 8 mars 2017 https://www.ladepeche.fr/article/2016/03/08/2299605-cybercriminalite-coute-3-36-milliards-euros-entreprises-francaises.html
27. MANYIKA J. et ROXBURGH C. *The great transformer: the impact of Internet on economic growth and prosperity*, McKinsey Global Institute, October 2011 https://www.mckinsey.com/~/media/McKinsey/Industries/High%20Tech/Our%20Insights/The%20great%20transformer/MGI_Impact_of_Internet_on_economic_growth.ashx
28. INTERNET ASSOCIATION, *New Report calculates the size of the Internet Economy*, 10 décembre 2015 https://internetassociation.org/121015econreport/
29. GLOBAL FINANCIAL INTEGRITY, *Transnational crime and the developing world*, Mars 2017 http://www.gfintegrity.org/wp-content/uploads/2017/03/Transnational_Crime-final.pdf
30. NATIONAL CRIME AGENCY, *Cyber crime assessment 2016*, 7 juillet 2016 http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file
31. JUNIPER RESEARCH, *Cybercrime to cost global business over $8 trillion in the next 5 years*, 30 mai 2017 https://www.juniperresearch.com/press/press-releases/cybercrime-to-cost-global-business-over-$8-trn
32. CYBERSECURITY VENTURES, *Cybercrime Damages $6 Trillion by 2021,* 16 Octobre 2017 https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
33. CGI, *The cyber-value connection* https://www.cgi.com/sites/default/files/2018-08/cybervalueconnection_full_report_final_lr.pdf
34. KAMIYA, S et all. *What is the Impact of Successful Cyberattacks on Target Firms* ?, 7 mars 2018 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3135514
35. CENTRIFY et PONEMON, *The impact of data breaches on reputation & share value*, Mai 2017 https://www.centrify.com/media/4772757/ponemon_data_breach_impact_study_uk.pdf
36. AMIR E. et LEVI S. et LIVNE,T., *Do firms underreport information on cyber-attacks ? Evidence from capital markets*, Mai 2017 https://sites.insead.edu/facultyresearch/research/file.cfm?fid=60951
37. NUSCA, A. *Equifax Stock has plunged 18,4% since it revealed massive breach*, 11 septembre 2017. http://fortune.com/2017/09/11/equifax-stock-cybersecurity-breach/
38. MARCOGLIESE,P et MUKHI R., *Untangling the Tangled Web of cybersecurity disclosure requirements: a practical guide*, 17 juin 2018 https://corpgov.law.harvard.edu/2018/06/17/untangling-the-tangled-web-of-cybersecurity-disclosure-requirements-a-practical-guide/

39. SOLOMON C et all, *Failure to Disclose a cybersecurity breach*, 17 mai 2018.
https://corpgov.law.harvard.edu/2018/05/17/failure-to-disclose-a-cybersecurity-breach/#more-106859
40. PONEMON Institute et ACCENTURE, *2017 Cost of cybercrime study*
https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
41. BARETT, B. *The wild inner workings of a billion-dollar hacking group*, 8 janvier 2018.
https://www.wired.com/story/fin7-wild-inner-workings-billion-dollar-hacking-group/
42. DEPARTEMENT OF JUSTICE, *Three members of notorious international cybercrime group "fin7" in custody for role in attacking over 100 US companies*, 1 aout 2018
https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100
43. FIREEYE, *On the hunt for FIN7: Pursuing an enigmatic and evasive global criminal operation*, 1 aout 2018.
https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html
44. LE MONDE, *Les Etats-Unis accusent trois ukrainiens d'avoir piraté 15 millions de cartes de crédit*, 2 aout 2018
https://www.lemonde.fr/pixels/article/2018/08/02/les-etats-unis-accusent-trois-ukrainiens-d-avoir-pirate-15-millions-de-cartes-de-credit_5338611_4408996.html
45. https://www.statista.com/chart/12707/largest-known-crypto-currency-thefts/
46. FIREEYE, *Unsealing the deal : cyber threats to mergers and acquisitions persist in a hot market,* 23 aout 2016
https://www.fireeye.com/blog/threat-research/2016/08/unsealing_the_deal.html
47. FIREEYE, *Hacking the street? FIN4 likely playing the market,* 2014.
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-fin4.pdf
48. LYNCH, S et MENN J., *Exclusive : SEC hunts hackers who stole corporate emails to trade stocks*, 23 juin 2015
https://www.reuters.com/article/us-hackers-insidertrading/exclusive-sec-hunts-hackers-who-stole-corporate-emails-to-trade-stocks-idUSKBN0P31M720150623?feedType=RSS&feedName=topNews
49. SEC vs JONATHAN LY
https://www.sec.gov/litigation/complaints/2016/comp-pr2016-256.pdf
50. SEC vs LOHUS HAAVEL & VIISEMANN, OLIVER PEEK, and KRISTJAN LEPIK
https://www.sec.gov/litigation/complaints/comp19450.pdf
51. RAJ CHANDEL'S BLOG, *5 ways to crawl a website*, 16 juillet 2017
http://www.hackingarticles.in/5-ways-crawl-website/
52. DEPARTMENT OF JUSTICE, *hackers sentenced to 30 months in prison for role in largest known computer hacking and securities fraud scheme*, 22 mai 2017
https://www.justice.gov/usao-nj/pr/hacker-sentenced-30-months-prison-role-largest-known-computer-hacking-and-securities
53. SEC vs DUBOVOY and all
https://www.sec.gov/litigation/complaints/2015/comp-pr2015-163.pdf
54. SEC, *SEC charges nine additional defendants in hacked news release*, 18 février 2016
https://www.sec.gov/litigation/litreleases/2016/lr23471.htm
55. SEC, *traders agrees to settle claims relating to hacked news release scheme; SEC's recovery to date in connection with the scheme exceeds $52 million*, 4 mai 2016
https://www.sec.gov/litigation/litreleases/2016/lr23530.htm
56. ASIC, *18-136MR IT consultant charged with gaining unauthorized access to dat and insider trading*, 14 mai 2018.
https://asic.gov.au/about-asic/media-centre/find-a-media-release/2018-releases/18-136mr-it-consultant-charged-with-gaining-unauthorised-access-to-data-and-insider-trading/

57. DEPARTMENT OF JUSTICE, *Five individual charged with participating in three insider trading schemes generating more than $5 million I profits on inside information misappropriated from an investment bank*, 16 aout 2017 https://www.justice.gov/usao-sdny/pr/five-individuals-charged-participating-three-insider-trading-schemes-generating-more-5
58. SEC vs IAT HONG, BO ZHENG, and HUNG CHIN https://www.sec.gov/litigation/complaints/2016/comp-pr2016-280.pdf
59. SEC, *SEC chairman clayton issues statement on cybersecurity*, 20 septembre 2017 https://www.sec.gov/news/press-release/2017-170
60. SEC, *Testimony on Oversight of the US SEC,* 21 juin 2018 https://www.sec.gov/news/testimony/testimony-oversight-us-securities-and-exchange-commission#_ftn1
61. ROBERTS, JJ. *Fake SEC emails targets execs for inside information*, 7 mars 2017 http://fortune.com/2017/03/07/sec-phishing/
62. FIREEYE, *FIN7 spear phishing campaign targets personnel involved in SEC filings*, 7 mars 2017 https://www.fireeye.com/blog/threat-research/2017/03/fin7_spear_phishing.html
63. TALOS, *Spoofed SEC emails distribute evolved DNSMssenger*, 11 octobre 2017 http://blog.talosintelligence.com/2017/10/dnsmessenger-sec-campaign.html
64. https://wraithhacker.com/2017/10/11/more-info-on-evolved-dnsmessenger/
65. SPRING, T. *New Fileless attack using dns queries to carry out powershell commands*, 4 mars 2017 https://threatpost.com/new-fileless-attack-using-dns-queries-to-carry-out-powershell-commands/124078/
66. REUTERS, *Exclusive: NASDAQ hackers spied on company boards*, 20 octobre 2011 https://www.reuters.com/article/us-nasdaq-hacking-idUSTRE79J84T20111020
67. ARSTECHNICA, *How elite hackers (almost) stole the NASDAQ*, 17 juillet 2014 https://arstechnica.com/information-technology/2014/07/how-elite-hackers-almost-stole-the-nasdaq/
68. REDOWL, *Monetizing the Insider* http://itzashita.ru/wp-content/uploads/2017/05/RedOwl_Intsights_Report.pdf
69. SIFMA CYBERSECURITY, *Insider threat best practices guide*, 2nd edition, Février 2018 https://www.sifma.org/wp-content/uploads/2018/02/insider-threat-best-practices-guide.pdf
70. REPKNIGHT, *Securing the Law Firm: Dark Web footprint analysis of 500 UK legal firms*, janvier 2018 https://www.repknight.com/wp-content/uploads/2018/01/White-Paper-Securing-the-Law-Firm-January-2018-Website-LM.pdf
71. SECURITYWEEK, *Hackers will break into email, social media accounts for just $129*, 6 avril 2016 https://www.securityweek.com/hackers-will-break-email-social-media-accounts-just-129
72. UNDERNEWS, *Telegram, le nouveau médium de choix de la cybercriminalité*, 9 mai 2018 https://www.undernews.fr/hacking-hacktivisme/telegram-le-nouveau-medium-de-choix-de-la-cybercriminalite.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+undernews%2FoCmA+%28UnderNews%29
73. CPR*, Telegram: cyber crime's channel of choice,* https://research.checkpoint.com/telegram-cyber-crimes-channel-choice/
74. SEC vs JUN YING https://www.sec.gov/litigation/complaints/2018/comp-pr2018-40.pdf
75. MARKETWATCH, *Short seller muddy waters renews claims of St. Jude Medical cyber vulnerabilities*, 19 octobre 2016. https://www.marketwatch.com/story/short-seller-muddy-waters-renews-claims-of-st-jude-medical-cyber-vulnerabilities-2016-10-19
76. THE WASHINGTON POST, The cybersecurity 202: a wake up call. OPM data stolen years ago surfacing now in financial fraud case, 20 juin 2018

https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/06/20/the-cybersecurity-202-a-wake-up-call-opm-data-stolen-years-ago-surfacing-now-in-financial-fraud-case/5b2924ca1b326b3967989b66/?noredirect=on&utm_term=.e1356c6af0a1

77. https://data.sca.isr.umich.edu/survey-info.php.
78. CNBC, *Thomson reuters gives elite traders early advantage*, 12 juin 2013 https://www.cnbc.com/id/100809395
79. GARTNER, *Gartner says 8,4 Billion connected things will be in use in 2017*, up 31 percent from 2016, 7 février 2017 https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016
80. HAGER, S. *Les voyageurs d'affaire, portes d'entrée des hackers* . Option Finance n°1467. 18 juin 2018
81. TECHRADARPRO, *why you should avoid hotel Wi-Fi like the plague*, 7 mars 2018 https://www.techradar.com/news/networking/wi-fi/why-you-should-avoid-hotel-wi-fi-like-the-plague-1292555/2
82. SECURITY RESEARCH LABS, *USB peripherals can turn against their users* https://srlabs.De/bites/usb-peripherals-turn/
83. KHANDELWAL S., *Hackers can silently control Siri, Alexa & Other voice assistants using ultrasound*, 6 septembre 2017 http://thehackernews.com/2017/09/ai-digital-voice-assistants.html
84. SEC vs JOSEPH P. WILLNER https://www.sec.gov/litigation/complaints/2017/comp-pr2017-202.pdf
85. SEC vs IDRIS D.MUSTAPHA https://www.sec.gov/litigation/complaints/2016/comp-pr2016-127.pdf
86. SEC vs IGORS NAGAICEVS https://www.sec.gov/litigation/complaints/2012/comp22238.pdf
87. SEC vs BROCO INVESTMENTS, INC and VALERY MALTSEV https://www.sec.gov/litigation/complaints/2010/comp21452.pdf
88. LIPOVSKY R., *Corkow: analysis of a business-oriented banking Trojan*, 27 février 2014. https://www.welivesecurity.com/2014/02/27/corkow-analysis-of-a-business-oriented-banking-trojan/
89. GROUP-IB REPORT: *Analysis of attacks against trading and bank card systems* https://www.group-ib.ru/brochures/Group-IB-Corkow-Report-EN.pdf
90. BOUTIN, JI et CHEREPANOV, A. *Modern attacks against Russian financial institutions*, Virus bulletin conference October 2016 https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Boutin-Cherepanov.pdf
91. POISTIVE TECHNOLOGIES, *Cobalt strikes back: an evolving multinational threat to finance*, 1 aout 2017 http://blog.ptsecurity.com/2017/08/cobalt-group-2017-cobalt-strikes-back.html
92. ROMANIA INSIDER, *Romanian financial institutions targeted by big cyber-attacks*, 20 aout 2018 https://www.romania-insider.com/financial-institutions-cyber-attacks/
93. DEPARTMENT OF JUSTICE, *Attorney General and Manhattan US Attorney announce charges stemming from massive network intrusions at US Financial Institutions, US Brokerage firms, Major News Publication and other companies*, 10 novembre 2015 https://www.justice.gov/opa/pr/attorney-general-and-manhattan-us-attorney-announce-charges-stemming-massive-network
94. REUTERS, *UPDATE 4-US charges three in huge cyberfraud targeting JPMorgan*, others, 10 novembre 2015 https://www.reuters.com/article/hacking-indictment-idUSL1N13518P20151110
95. SEC vs JOSHUA SAMUEL AARON, GERY SHALON, and ZVI ORENSTEIN. https://www.sec.gov/litigation/complaints/2015/comp-pr2015-152.pdf
96. REUTERS, HongKong police struggle to stop hacking spree, 15 février 2017

https://in.reuters.com/article/cyber-brokerages-hongkong/hong-kong-police-struggle-to-stop-brokerage-hacking-spree-idINKBN15U0BA

97. HONGKONG CASE LAW*, fast track holdings ltd vs BOCI securities ltd and others*, 12 novembre 2016 https://www.hongkongcaselaw.com/fast-track-holdings-ltd-v-boci-securities-ltd-and-others/
98. SFC, *SFC notifies the industry of cybersecurity review on internet/mobile trading systems*, 13 octobre 2013 https://www.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=16EC46
99. SFC, *Consultation paper on proposals to reduce and mitigate hacking risks associated with Internet trading*, Mai 2017 https://www.sfc.hk/edistributionWeb/gateway/EN/consultation/openFile?refNo=17CP4
100. SOUTH CHINA MORNING POST, *SFC orders tighter safeguards to stop hackers invading online trading accounts*, 27 octobre 2017 https://www.scmp.com/business/article/2117363/sfc-orders-tighter-safeguards-stop-hackers-invading-online-trading-accounts
101. SFC, *Circular to intermediaries receiving client orders through instant messaging*, 4 mai 2018 https://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=18EC30
102. ESET, *State of cybersecurity in APAC: small businesses, big threats* https://www.welivesecurity.com/wp-content/uploads/2017/10/State-of-cybersecurity-in-APAC_Small-Businesses-Big-Threats.pdf
103. KREBSON SECURITY, *Target hackers broke in via HVAC Company*, 14 février 2014 https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company
104. HERNANDEZ, A. *Are you trading stocks securely? Exposing security flaws in trading technologies*. IOActive, juillet 2018 https://ioactive.com/wp-content/uploads/2018/08/Are-You-Trading-Stocks-Securely-Exposing-Security-Flaws-in-Trading-Technologies.pdf
105. https://www.ft.com/content/d81f96ea-d43c-11e7-a303-9060cb1e5f44
106. KOPPENHEFFER, *M. Everything you need to know about the Knight Capital Meltdown*, 14 septembre 2012. https://www.fool.com/investing/general/2012/09/14/everything-you-need-to-know-about-the-knight-capit.aspx
107. THE TECHNOLOGY EVANGELIST, *Security: DARPA, HFT & FINANCIAL MARKETS*, 18 décembre 2017 https://technologyevangelist.co/2017/12/18/security-darpa-hft-financial-markets
108. SNYDER, *B. Hackers find new way to cheat on Wall Street—to everyone's peril*, INFOWORLD, 6 janvier 2011 https://www.infoworld.com/article/2624981/network-monitoring/hackers-find-new-way-to-cheat-on-wall-street----to-everyone-s-peril.html
109. THE HISTORY OF PRESS*, Napoleon is dead! The great stock exchange fraud of 1814* https://www.thehistorypress.co.uk/articles/napoleon-is-dead-the-great-stock-exchange-fraud-of-1814/
110. LE MONDE, *les grandes entreprises de la Silicon Valley se rencontrent pour parler de la désinformation*, 24 aout 2018 https://www.lemonde.fr/pixels/article/2018/08/24/les-grandes-entreprises-de-la-silicon-valley-se-rencontrent-pour-parler-de-la-desinformation_5345665_4408996.html
111. MINISTERE DE LA CULTURE, *les enjeux de la loi contre la manipulation de l'information*, 4 juillet 2018. http://www.culture.gouv.fr/Actualites/Les-enjeux-de-la-loi-contre-la-manipulation-de-l-information
112. FUTURISM*, Ethereum lost $4 Billion in market value due to fake "fatal car crash"*, 27 juin 2017 https://futurism.com/ethereum-lost-4-billion-in-market-value-due-to-fake-fatal-car-crash/
113. SEC vs MARK S. JAKOB https://www.sec.gov/litigation/litreleases/lr16671.htm
114. DUFFY, *A. Fake press release wipes $314 million of Whitehaven*, Australian Mining, 7 janvier 2013 https://www.australianmining.com.au/news/fake-press-release-wipes-314-million-off-whitehaven/
115. MARTIN, B et SPENCE, P. *G4S shares knocked by elaborate hoax regarding company's finances*, 12 novembre 2014. http://www.telegraph.co.uk/finance/markets/11226463/G4S-shares-knocked-by-elaborate-hoax-regarding-companys-finances.html

116. ANONYME, *Prank the pranksters! Playing around with information and fakes in the age of immaterial capitalism* https://foolcapitalism.espivblogs.net/files/2015/10/PrankThePrankster.pdf
117. THOMPSON M et KOTTASOVA, I, *How a big Italian bank was slammed by an hoax*, 24 avril 2015 https://money.cnn.com/2015/04/24/investing/italian-bank-hoax/
118. https://www.linkiesta.it/it/article/2015/04/24/il-finto-comunicato-che-ha-fatto-tremare-il-titolo-di-intesa-sanpaolo/25628/
119. http://www.ilgiornale.it/news/politica/email-far-crollare-mercato-i-no-tav-attaccano-banca-italiana-1120580.html
120. THE GUARDIAN, *Twitter's shares jump after fake story company's $31bn takeover offer*, 14 juillet 2015 https://www.theguardian.com/technology/2015/jul/14/twitter-shares-fake-story-bloomberg
121. FILIPPONE D., *Vinci dégringole en bourse suite à un hoax*, 23 novembre 2016 https://www.lemondeinformatique.fr/actualites/lire-vinci-degringole-en-bourse-suite-a-un-hoax-66589.html
122. JACQUE, P. *Comment le groupe Vinci victime d'un « hoax » a chuté en Bourse*, 23 novembre 2016 https://www.lemonde.fr/economie-francaise/article/2016/11/23/comment-le-groupe-vinci-victime-d-un-hoax-a-chute-en-bourse_5036269_1656968.html
123. AMF, *l'AMF présente l'avancement de ses travaux à la suite de la diffusion d'une fausse information relative au titre Vinci*, 23 février 2017 https://www.amf-france.org/Actualites/Communiques-de-presse/AMF/annee-2017.html?docId=workspace%3A%2F%2FSpacesStore%2Ffba06651-ed84-4e46-a9db-1876b4330712
124. SELYUKH, *A. Hackers send fake market moving AP tweet on White House explosions*, 23 avril 2013 https://www.reuters.com/article/net-us-usa-whitehouse-ap/hackers-send-fake-market-moving-ap-tweet-on-white-house-explosions-idUSBRE93M12Y20130423
125. https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/?utm_term=.e0629cdeaadf
126. SEC vs JAMES ALAN CRAIG https://www.sec.gov/litigation/complaints/2015/comp-pr2015-254.pdf
127. https://seekingalpha.com/article/2274553-cynk-technology-promoters-push-market-cap-to-655-million-despite-39-in-assets-and-no-revenue-100-percent-downside?page=1
128. http://promotionstocksecrets.com/cynk-aftermath-putting-together-pieces-puzzle/
129. SEC vs PHILIP THOMAS KUEBER https://www.sec.gov/litigation/complaints/2015/comp-pr-2015-157.pdf
130. CNET, *Facebook deleted 583 million fake accounts in the first three months of 2018*, 15 mai 2018 https://www.cnet.com/news/facebook-deleted-583-million-fake-accounts-in-the-first-three-months-of-2018/
131. NEWBERG M. *As many as 48 million Twitter accounts aren't people, says study*. 10 mars 2017 https://www.cnbc.com/2017/03/10/nearly-48-million-twitter-accounts-could-be-bots-says-study.html
132. *The DARPA Twitter Bot Challenge*, 21 avril 2016 https://arxiv.org/abs/1601.05140
133. HUET S., *Sur twitter le faux plus fort que le vrai*, 8 mars 2018. http://huet.blog.lemonde.fr/2018/03/08/sur-twitter-le-faux-plus-fort-que-le-vrai/
134. SEC, *Updated investor Alert: Social Media and investing—Stock Rumors*, 6 février 2017 https://www.sec.gov/oiea/investor-alerts-bulletins/ia_rumors.html
135. SEC vs NAUMAN A. ALY https://www.sec.gov/litigation/complaints/2016/comp-pr2016-95.pdf
136. SEC vs ROBERT W.MURRAY https://www.sec.gov/litigation/complaints/2017/comp23836.pdf
137. SEC vs PTG CAPITAL PARTNERS, NEDKO NEDEV et all https://www.sec.gov/litigation/complaints/2015/comp-pr2015-110.pdf

138. http://materials-risk.com/livestock-prices-top-10-important-drivers/
139. LEXPRESS, *Standard&Poor's sanctionnée pour avoir dégradé la France par erreur*, 5 juin 2014 https://lexpansion.lexpress.fr/actualite-economique/standard-poor-s-reprimande-pour-avoir-degrade-la-france-par-erreur_1548720.html
140. NICOLAS, *A. Les trois plus grosses bourdes des agences de notation*, 11 novembre 2011 https://www.francetvinfo.fr/economie/bourse/marches/les-trois-plus-grosses-bourdes-des-agences-de-notation_25721.html
141. FINEXTRA, '*Fake data' will make banks vulnerable-Accenture*, 20 avril 2018 https://www.finextra.com/newsarticle/31978/fake-data-will-make-banks-vulnerable---accenture?utm_medium=dailynewsletter&utm_source=2018-4-23&member=42526
142. https://www.youtube.com/watch?v=cQ54GDm1eL0
143. https://goberoi.com/exploring-deepfakes-20c9947c22d9
144. https://www.deepfakes.club/best-hardware-software-deepfakes/
145. https://www.alanzucconi.com/2018/03/14/introduction-to-deepfakes/
146. TUAL, *M. Du porno aux fausses informations, l'intelligence artificielle manipule désormais la vidéo*, 8 février 2018 https://www.lemonde.fr/pixels/article/2018/02/04/du-porno-aux-fausses-informations-l-intelligence-artificielle-manipule-desormais-la-video_5251535_4408996.html
147. COURRIER INTERNATIONAL, Vous n'avez encore rien vu ! Quand la réalité s'effondre, Jeudi 23 Aout 2018 http://lirelactu.fr/source/courrier-international/b64b4654-ada4-4f5a-b0d6-4966dea55a41
148. FINANCIAL TIMES, *if you thought fake news was a problem, wait for deepfakes* https://www.ft.com/content/8e63b372-8f19-11e8-b639-7680cedcc421
149. OICV-IOSCO, Cyber-crime, securities markets and systemic risk, 16 juillet 2013 https://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf
150. PROLEXIC, *DDOS Attacks against global markets*, 2014 https://www.akamai.com/de/de/multimedia/documents/content/ddos-attacks-against-global-markets-white-paper.pdf
151. HOFMANS,T. *Teenager suspected of crippling Dutch banks with DDoS attacks*, 8 février 2018 https://www.computerweekly.com/news/252434665/Teenager-suspected-of-crippling-Dutch-banks-with-DDoS-attacks
152. FINANCIAL TIMES, *HongKong echange hit by hackers* https://www.theglobeandmail.com/report-on-business/international-business/hong-kong-exchange-hit-by-hackers/article599797/
153. BENNET C, *Hackers breach the warsaw stock exchange*, The Hill, 24 octobre 2014 http://thehill.com/policy/cybersecurity/221806-hackers-breach-the-warsaw-stock-exchange
154. USA vs VLADIMIR DRINKMAN, ALEKSANDR KALININ et all https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/02/18/drinkman_vladimir_et_al_indictment_comp.pdf
155. DEPARTMENT OF JUSTICE, *Russian national charged in largest known data breach prosecution extradited to United States*, 17 février 2015 https://www.justice.gov/opa/pr/russian-national-charged-largest-known-data-breach-prosecution-extradited-united-states
156. GOODIN, D. *"NASDAQ is owned" five men charged in largest financial hack ever*, 25 juillet 2013 https://arstechnica.com/information-technology/2013/07/nasdaq-is-owned-five-men-charged-in-largest-financial-hack-ever/
157. WEF,*The new physics of Financial Services*, Aout 2018 http://www3.weforum.org/docs/WEF_New_Physics_of_Financial_Services.pdf
158. ZORZ, Z. *The percentage of open source code in proprietary apps in rising*, 22 mai 2018 https://www.helpnetsecurity.com/2018/05/22/open-source-code-security-risk/

159. ECHENNE, F. Les risques d'une circulation non maîtrisée des flux financiers et informationnels sur Internet, Cahiers de la sécurité et de la Justice n°42, 8 juin 2018
160. Nessim Aît-Kacimi, *Comment les cyberpirates ukrainiens font trembler WallStreet*, Article des Echos, 13 mars 2019
161. https://www.lesechos.fr/2017/10/le-cyber-est-un-meta-risque-qui-touche-tous-les-metiers-de-lentreprise-184557
162. https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline
163. https://www.securityinsider-wavestone.com/2016/06/retour-sur-laffaire-swift-synthese-des.html
164. https://www.afg.asso.fr/wp-content/uploads/2018/12/2018_10_18_Cybersécurité_Enquete-AFG_octobre-2018_site.pdf
165. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf
166. https://www.bis.org/cpmi/publ/d146.pdf
167. https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf
168. https://www.swift.com/resource/how-cyber-attackers-could-target-worlds-financial-markets
169. https://www.sec.gov/news/press-release/2018-22
170. https://www.sec.gov/news/press-release/2018-71
171. Rapports financiers annuels :
https://www.saint-gobain.com/sites/sgcom.master/files/fy-2017-fra_a.pdf
http://s1.q4cdn.com/714383399/files/oar/2017/AnnualReport2017/AnnualReport2017flat/docs/FedEx_2017_Annual_Report.pdf
https://www.maersk.com/-/media/ml/about/sustainability/20180209-a-p-moller-maersk-annual-report.pdf
https://ir.mondelezinternational.com/news-releases/news-release-details/mondelez-international-reports-2017-results
http://s21.q4cdn.com/488056881/files/doc_financials/2017/2017-Form-10-K_FINAL-wo-Exhibits_Filed-022718.pdf
172. https://www.statista.com/chart/12707/largest-known-crypto-currency-thefts/
173. KIRK S. Satellites and sensitive sheep blur insider trading ,Financial Times, 29 Novembre 2017.
174. https://www.zdnet.com/article/black-hat-hackers-white-collar-criminals-snuggle-up-to-operate-insider-trading-schemes/
175. https://www.fbi.gov/news/stories/chinese-hackers-indicted-122018
176. https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion
177. https://www.theverge.com/2018/8/22/17716622/sec-business-wire-hack-stolen-press-release-fraud-ukraine
178. https://www.sec.gov/news/press-release/2019-1
179. https://www.sec.gov/litigation/complaints/2019/comp-pr2019-1.pdf
180. https://www.zdnet.com/article/oklahoma-gov-data-leak-exposes-millions-of-department-files-fbi-investigations/
181. https://www.lemondeinformatique.fr/actualités/lire-shodan-moteur-de-recherche-total-de-l-internet-71919.html
182. https://www.amf-france.org/Actualites/Communiques-de-presse/AMF/annee-2018?docId=workspace%3A%2F%2FSpacesStore%2F3d58f35b-f448-438e-9923-cd6e8e903fc0
183. https://www.timesofmalta.com/articles/view/20190225/local/how-bov-hackers-got-away-with-13-million.702800
184. https://asic.gov.au/online-services/service-availability/scams-targeting-asic-customers/
185. https://www.darkreading.com/vulnerabilities---threats/new-report-details-rise-spread-of-email-based-attacks/d/d-id/1333375
186. https://www.bleepingcomputer.com/news/security/over-80-percent-of-all-phishing-attacks-targeted-us-organizations/
187. https://www.gao.gov/assets/700/694158.pdf
188. https://yle.fi/uutiset/osasto/news/cyber-attack_shuts_finnish_ministry_jobs_site/10518762
189. http://www.globalsecuritymag.fr/Les-cyberattaques-visant-les,20190306,85113.html
190. http://www.bromium.com/social-media-platforms-cybercrime-economy/
191. http://globbsecurity.fr/office-365-ligne-de-mire-cybercriminels-44303/

192. https://www.solutions-numeriques.com/cyberattaques-office-365-et-google-g-suite-de-plus-en-plus-vises/
193. https://www.pcworld.com/article/3235484/what-the-kaspersky-antivirus-hack-really-means.html
194. https://www.lemonde.fr/pixels/article/2018/10/04/les-pays-bas-revelent-une-operation-d-espionnage-russe-sur-leur-territoire_5364712_4408996.html
195. https://english.defensie.nl/downloads/publications/2018/10/04/gru-close-access-cyber-operation-against-opcw
196. https://www.lemonde.fr/pixels/article/2018/10/04/espionnage-la-chine-accusee-d-avoir-installe-des-micropuces-dans-des-serveurs-utilises-par-apple-et-amazon_5364769_4408996.html
197. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
198. https://www.zdnet.com/article/crims-not-spooks-dominate-cybersecurity-threats-sophos-ceo/
199. https://www.difesaesicurezza.com/en/cyber-en/the-cybercrime-group-carbanak-aka-cobalt-and-fin7-is-not-yet-defeated/
200. https://securelist.com/ksb-cyberthreats-to-financial-institutions-2019-overview-and-predictions/88944/
201. https://www.lesechos.fr/2018/03/cybercriminalite-le-cerveau-du-gang-des-carbanak-arrete-987505
202. https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain
203. https://news.8btc.com/alert-lazarus-hacker-group-continues-targeting-crypto-using-faked-trading-software
204. https://www.smh.com.au/national/nsw/jonathan-moylan-avoids-jail-term-for-fake-anz-media-release-about-whitehaven-coal-20140725-zwwe7.html
205. https://www.smh.com.au/business/dont-believe-the-hype-over-the-cost-of-whitehaven-hoax-20130115-2crh1.html
206. https://www.reuters.com/article/us-fingerprint-samsung/swedish-tech-company-caught-in-hoax-samsung-bid-idUSBRE99A07N20131011
207. https://qz.com/134493/one-fake-press-release-created-200-million-today-and-another-one-made-it-disappear/
208. https://www.reuters.com/article/immunovaccine-regulator-hoax/trades-in-immunovaccine-shares-to-be-undone-after-hoax-spurs-30-pct-jump-idUSL1N0W523G20150303
209. https://www.benzinga.com/news/15/02/5283736/immunovaccine-up-24-on-deal-with-gilead-sciences
210. https://www.fnlondon.com/articles/blackrock-targeted-by-fake-ceo-letter-20190116
211. https://www.lemonde.fr/pixels/article/2019/02/07/whatsapp-supprime-2-millions-de-comptes-par-mois-pour-lutter-contre-les-fausses-informations_5420513_4408996.html
212. https://edition.cnn.com/2019/01/28/tech/deepfake-lawmakers/index.html.
213. https://www.washingtonexaminer.com/news/white-house/the-deep-fake-threat
214. https://www.amf-france.org/Reglementation/Dossiers-thematiques/Fintech/Vers-un-nouveau-regime-pour-les-crypto-actifs-en-France
215. https://www.vox.com/2018/1/23/16923276/facebook-twitter-russia-interference-congress-release-the-memo
216. https://siecledigital.fr/2019/07/23/scandale-equifax-la-societe-recoit-une-amende-de-700-millions-de-dollars
217. https://www.journaldugeek.com/2019/07/25/facebook-amende-record-sans-consequence/
218. https://www.fsb.org/2018/11/cyber-lexicon/
219. https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf
220. https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf
221. https://www.finextra.com/newsarticle/34352/hong-kong-exchange-suffers-cyber-attack

INDEX

accounting firms 19
activist 37, 38, 39, 40, 41, 42
activists 50
algorithmic trading 35
algorithms 35, 36, 46
Aly 47
AMF 8, 24, 44, 49
anonymity on the internet 42
ANSSI 8
antivirus software vendors 28
Anunak 33
APT 11, 53
APT10 20
APT38 33
artificial intelligence 49
ASIC 24
asset class 27, 48
Associated Press 44
attack surface 29
Audience 44
Australia 21, 38
automation 46, 49
AVON 47
Banca Intesa Sanpaolo 40
Bangladesh 18
Bank of Valetta 24
Banque de France 8
big data 19
biotech 19
BlackRock 42
Bloomberg 34, 37, 38, 39, 41, 49
botnets 25
bots 46
Broco 31
business travellers 27
Business Wire 20
Canada 39
Carbanak 33
China 29
Chinese hackers 20, 22, 34
Cloud 27
Cobalt 33
connected objects 13, 27
consultancy firms 19
consulting banks 19
Corkow 32
Craig 44
credential stuffing 25
credibility 49
cryptocurrencies 42
cryptocurrency 10, 18

cyber
component ... 8, 29
cyber event ... 11
cyber espionage ... 28
Cyber Expert Group ... 8
cyber resilience ... 5
cyber scams ... 10
cyber unit ... 9
cybercrime ... 5
cyberfraud ... 5
cyberisation ... 8
cybersecurity ... 5
cyberterrorism ... 50
CYNK ... 45
Dark Web ... 9, 25
DARPA ... 36, 46
data integrity ... 48
dataroom providers ... 19
DDoS ... 50
deepfake ... 49
destabilisation ... 37
dissemination of false information ... 36, 46
dissemination of false or misleading information ... 8
dissemination of financial information ... 43
Distributed Ledger Technology ... 9
DoS ... 50
Dow Jones ... 38
drones ... 19
economic data ... 27
economic espionage ... 20, 29
economic indicators ... 27
EDGAR ... 22, 23, 47
email-based attacks ... 24
Emulex ... 38
Energobank ... 32
Equifax ... 18, 26
ESMA ... 8
Ethereum ... 36
European Systemic Group ... 8
Expedia ... 20
Facebook ... 18
fake data ... 48
fake email ... 42
fake news ... 36, 48
fake tender offer ... 47
fake tweets ... 44
false filing ... 47
false or misleading information ... 8
false press release ... 38, 39, 40, 41, 44
FBI ... 5, 23, 38, 44
FDA ... 45
FED ... 49
FIN4 ... 19

FIN7 ..... 18, 23
financial information provider 37, 38
financial information providers 19, 49
financial instruments 27
Financial Stability Board 8
Fingerprint Cards 39
Finland 27
FITBIT 47
forums 19, 25
G4S 39
G7 8
GDP 12
General Data Protection Regulation 11
Getco 35
hacktivists 33
high-frequency trading 35
hoax 36, 37, 39, 40, 42, 43
Hong Kong 34, 50
ICO 9
identity theft 26
Ieremenko 21, 22
Immunovaccine 39
impact on the share price of listed companies 11
Initial Coin Offering 9
inside information 7, 19, 25
insider 7
insider risk 19, 25
inspections 8
Integrated Device Technology, Inc 47
Internet Wire 38
investigations 7
Investigations and Inspection Division 7
IOSCO 8, 50
IP address 21, 47
IT consultant 21, 22
IT technician 20, 22
Italy 40
JP Morgan 31
Kaspersky 28
Knight Capital 35
law firms 19, 25
layering/spoofing 29
Lazarus 33
Lohmus 20
loss actually incurred 43
loss of market capitalisation 36, 43
Ly 20
machine learning 49
Maltsev 31
management companies 8
Man-In-The-Middle 34
mapping 27, 33, 48
Mark Jakob 38

MarketWire 21
massive data leak 26
merger and acquisition 19
mergers and acquisitions 22
microchips 29
misinformation 37, 49
mobile trading systems 34
Muddy Waters 26, 44
Murray 47
Mustapha 31
Nagaicevs 31
Napoleon Bonaparte 36
Nasdaq 24
NASDAQ 50
Nedko Nedev 47
Netherlands 28
news agencies 44
NotPetya 17
Oakes 21
Obama 44
official channel for disseminating information 44
Oklahoma 23
organised criminal groups 33
organised cybercriminal groups 32
penny stocks 34
personal data loss 23, 25, 26, 31, 32
PETYA 17
phishing 19, 24, 25, 26
Prank the pranksters 39
price manipulation 7, 29
PRN 21
promotional campaign 45
public relations agencies 19
pump-and-dump 29, 31, 45, 46
rating agencies 37, 48
reputation 11
Reuters 37, 49
RIVAS 22
robot advisors 49
Rocky Mountain 47
rumour 41
rumours 46
Russian 28
Russian hackers 50
Sarepta Therapeutics 45
satellites 19
scarcity of data 11
SEC 9, 22, 23, 38, 44, 45, 47
Shalon 26, 31
SHODAN 23
social bots 46, 49
social media 28, 36, 46
spearphishing 24

St. Jude Medical 26
Standard & Poor's 48
stock market breaches 7
supply chain 5
Sweden 39
SWIFT 6
Syrian Electronic Army 44
targeted email campaign 24
Telegram. 25
Thomson Reuters 27
TOR 42
Tower Group 47
trading accounts 30, 31, 32, 34
trading applications 34
trading on instant messaging platforms 34
trading systems 33
translation agencies 19
Treasury Department 8
Turchynov 21
tweet 39
Twitter 37, 41, 46
Uber 11, 26
Ukranian hackers 21
USB 28
Vinci 36, 41, 43
Virtu Financial 35
voice controlled connected objects 28
VPN 42
Warsaw 50
WhatsApp 46
White House 44
Whitehaven Coal 38
Wi-Fi 28
Willner 30
Word 24
Yahoo 11, 26