Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

armasuisse Science and Technology
Cyber-Defence Campus

Master's Thesis

Disentangling the sources of cyber risk premia

Author
Nathan Monnet

Academic Supervisor
Prof. Julien Hugonnier

Company Supervisors
Dr. Alain Mermoud
Dr. Loïc Maréchal

A thesis submitted in fulfillment of the requirements for the Master degree in

Financial Engineering

August 13, 2024

Contents

List of Figures

List of Tables

Abstract

This thesis uses a methodology based on a machine learning algorithm to quantify firms' cyber risks based on their disclosures and a dedicated cyber corpus. The model can identify paragraphs related to determined cyber-attack types and accordingly attribute different related cyber scores to the firm. The cyber scores are unrelated to other firms' characteristics. Stocks with high cyber scores significantly outperform other stocks. The long-short cyber risk factors have positive risk premia, are robust to all factors' benchmarks, and help price returns. Furthermore, I suggest the market does not distinguish between different types of cyber risks but instead views them as a single, aggregate cyber risk.

Disclaimer regarding the use of generative AI: Chat GPT was used solely to enhance the text style throughout this paper. All original ideas and concepts presented are entirely my own. Most prompts followed the structure: "Correct and improve this sentence." Sentence-wise improvement and constant human supervision ensured that no irrelevant information, misinformation, or unsolicited information was introduced.

This document results from a research project funded by the Cyber-Defence Campus, armasuisse Science and Technology. I appreciate helpful comments from Prof. Julien Hugonnier and seminar participants at the Cyber Alp retreat 2024. The code and data are available at: https://github.com/nmonnet/disentangling-cyber-risk-premia

Chapter 1

Introduction

1.1 CYD Campus activity, technology monitoring, and finance

This thesis results from a collaboration between EPFL and the Cyber-Defence Campus (CYD Campus). The Cyber-Defence Campus (CYD Campus) was founded in January 2019 by armasuisse Science and Technology to enhance Switzerland's defense posture against cyber threats. In 2017, the head of the Federal Department of Defence, Civil Protection and Sport (DDPS) issued a cyber defense action plan to enhance the nation's cybersecurity. A key component of this Action Plan for Cyber-Defence (APCD) was the establishment of the CYD Campus, tasked with anticipating cyber developments, monitoring trends, and developing the necessary skills and technologies for effective cyber defense. The CYD Campus provides the DDPS with a platform for identifying and assessing technological, economic, and societal cyber trends. To facilitate collaboration with academia, government, and industry, the CYD Campus operates from three sites: its primary location in Thun (armasuisse Science and Technology), the EPFL in Lausanne, and near the ETH in Zurich. This strategic positioning enables the CYD Campus to efficiently build expertise and act as a nexus between the private sector, public sector, and academic community. Under the guidance of the Federal Council, the CYD Campus focuses on three main tasks: early identification of cyber trends, research and innovation in cyber technologies, and training of cyber specialists at various academic levels.

More specifically, this research arises from the Technology and Monitoring (TM) department of the CYD Campus, which aims to provide an anticipation and monitoring platform for cybersecurity technologies and the social impact of cyber threats. TM employs both qualitative and quantitative approaches to identify emerging cyber-technologies and firms. The former is done through scouting, and the latter through publicly available or private data analysis. TM also acts as a data aggregator, including that issued from the qualitative scouting, and is thus proprietary. This research uses quantitative finance methods to contribute to the objectives of the CYD Campus.

This research also arises in a more widespread and costly context for cyber incidents, where cyber-insurance contracts and cybersecurity solutions have become crucial for private and public organizations. These countermeasures, however, have difficult-to-estimate costs. This thesis uses

natural language processing, clustering methods, and state-of-the-art asset pricing techniques to disentangle and quantify the risk premia of various cyber threats.

As part of my involvement, I integrated the Technology Monitoring team as an intern. Within this framework, I was tasked with delivering a thesis focusing on assessing cyber risk in firms, using the market as a source of evidence and thus employing financial methods to gain insight. This thesis is intended to be repurposed as a publishable academic paper. Additionally, a portion of the code developed for this paper is slated to become a free-of-rights Python library, enhancing accessibility and utility for broader research and application. Furthermore, I had the opportunity to present my work and its relevance at the Cyber Alp Retreat. This event, held in Sachseln (Obwalden) at the end of June 2024, brought together Swiss Technology Observatory community members. DDPS, industry, and academia participants gathered to discuss current and future challenges and drivers in cyberspace over several days. Key topics such as data scouting and emergent technology such as Large Language Models or Quantum computing were discussed, showcasing the collaborative efforts and advancements in cyber defense.

1.2 Objective and findings

The main focus of this paper is to disentangle the different cyber risks faced by firms and the effects on expected returns through risk premia channels. To do this, I collect financial fillings, monthly returns, and other firm characteristics for over 7000 firms listed on US stock markets between January 2007 and December 2023. I use a neural network called "Paragraph Vector" in combination with the MITRE ATT&CK cybersecurity knowledgebase and clustering techniques to score each firm's filing based on its various types of cyber risk.

I find four types of cyber attacks emerge from the textual cluster structures of MITRE ATT&CK. I establish scores to quantify the similarity between the annual statements of firms, the 10-Ks, and the identified types of cyber attacks from the knowledgebase MITRE ATT&CK. I find that the four "cyber" scores present no correlation with standard firms' characteristics known to help price stock returns and weak correlations with textual non-semantic variables of the annual statement (the highest, 0.36, correlates with the length of section 1.A., in the 10-Ks). As previously observed in a study using the same neural network, the resulting aggregation of the various cyber scores shows increasing trends, with scores increasing by 0.04 from 2007 to 2023. I also find that specific industries from the Fama-French 12-industries classification display higher cyber scores, with Business Equipment and Telephone and Television Transmission being the highest.

I find that organizing firms into portfolios based on their cyber scores, with increasing cyber scores, results in progressively higher average excess returns. All average excess returns of all portfolios are statistically significant at the 1% level, and investing in a portfolio that enters a long (short) position in the top (bottom) cyber scores firm is statistically significant at the 5% level. The aforementioned results stay true at the 5% and 10% levels in the top portfolios after controlling for common risk factors.

The risk premia associated with the different types of cyber risk are also manifest at the 5% level in the cross-section with Fama and MacBeth (1973) regressions. Using additional pricing

factors related to cyber-based portfolios improves pricing ability. I demonstrate that joint alphas of various assets tend to decrease in Gibbons, Ross, and Shanken (1989) tests. Using the Bayesian approach of Barillas and Shanken (2018), I also demonstrate that the optimal subset of factors pricing stock returns invariably includes the cyber-based factors.

Additional tests reveal that, although various types of cyber risk exist, the market does not differentiate between them and perceives them as a single aggregate cyber risk. Finally, I conduct an event analysis to evaluate the performance of a cyber-based portfolio during the massive SolarWinds cyber attack in December 2020. Contrary to previous studies, no significant conclusions can be drawn from this event regarding the performance of my cyber-based portfolios in cyber-related crises.

The remainder of this work proceeds as follows. Chapter 2 introduces the related literature and develops hypotheses; Chapters 3 and 4 present the data and the methodology. Chapter 5 details the results, and Chapter 6 concludes.

Chapter 2

Literature Review

2.1 Asset Pricing

2.1.1 Factor models

Treynor (1962) proposes that the return of an asset should be proportional to its exposure to systematic risk, measured by a beta (a proportion factor to the systemic risk), thus emphasizing the trade-off between risk and return. Similarly, Sharpe (1964) develops the Capital Asset Pricing Model (CAPM). The model intends to explain the link between systematic risk and expected return for individual assets. Lintner (1965) provided more rigor to the theoretical frame of the CAPM, and Mossin (1966) introduced the model independently with a different approach, strengthening the foundation of the CAPM. The model states that the expected return of an asset is determined by the risk-free rate and a risk premium, which is the market excess return multiplied by the asset's beta coefficient.

However, the CAPM can be expanded to include multiple factors for pricing an asset's returns. With this idea, Ross (1976) proposes the Arbitrage Pricing Theory (APT). The APT states that the excess returns of a collection of assets can be written as:

$$R^e = \alpha + \beta \boldsymbol{F} + \epsilon \tag{2.1}$$

Where the vectors R^e contain the excess returns of the assets. The intercepts α represent the portion of the excess returns that can not be explained by the systematic risk factors included in the model, and $\mathbf{F}$ is the factor returns.

Additionally, the asset pricing literature introduces several factors sequentially to the market excess return. Fama and French (1992) add the market capitalization and the book-to-market as factors to predict returns. Carhart (1997) adds a momentum factor, which is a portfolio entering a long (short) position in assets that performed well (poorly) in the past. Fama and French (2015) extend this set of factors with two additional ones, investment and operating profitability, resulting in the five-factor model.

The framework introduced by the APT leads to the finding of numerous pricing factors through the literature, eventually creating a "factor zoo". However, caution is required since Harvey, Liu,

and Zhu (2016) shows that the reported factors in the literature usually display poor statistical scores when tested independently on out-of-sample, more recent returns.

2.1.2 Asset Pricing Tests

Different methods exist to assess the performance of a model (set of pricing factors). Fama and MacBeth (1973) apply a method involving two-step rolling regressions to simultaneously find both the beta and the risk-premium associated with each factor and further test their statistical significance. Gibbons et al. (1989) build a statistical score to test if the alphas of 2.1 are commonly zeros, thus implying that involved factors capture all the priced risk associated with the returns. Barillas and Shanken (2018) presented a method to test if a subset of factors is better at pricing factors than an alternative, more general set of factors.

2.2 Natural language processing and machine learning

Natural Language Processing (NLP) is a domain that crosses the field of Machine Learning (ML) and aims to produce methods that allow computers to assess linguistic data. In finance, NLP can be used to assess and take into account investors' or managers' opinions regarding an investment.

2.2.1 Sentiment analysis and text classification

Sentiment analysis, and more generally, text classification, consists of NLP methods that classify textual data into categories, such as positive/negative or theme-related ones. Those classifications aim to create scores that translate the human perception included in texts into meaningful quantities. Those scores can then be used as pricing factors or can help build them. Until recently, most of the methods used were dictionary-based. The dictionary-based method implies that to be classified into the category of a theme, a text must display multiple occurrences of words or n-grams (specific sequences of n words) associated with the theme. Those lists of theme-related words called dictionaries are built prior to the analysis and tend to be arbitrary.

Antweiler and Frank (2004) study more than 1.5 million messages posted on Yahoo! Finance and Raging Bull about the 45 companies in the Dow Jones Industrial Average and the Dow Jones Internet Index stock trading during the year 2000 to infer daily stock returns using the Naive Bayes algorithm. This dictionary-based method provides the probability of belonging to a category (in this case, "buy", "hold", "sell") given the vector of occurrences of words figuring in a previously constructed dictionary. From the proportion of classified messages in the three categories at different times, they construct several scores such as overall "bullishness" and "agreement". They find that an increase in forum activity precedes small negative returns on the following trading day. Furthermore, Disagreement among messages correlates with increased trading volume, especially for smaller trades, but higher disagreement leads to fewer trades the next day rather than more. Additionally, they find that forum activity is a reliable predictor of market volatility, both daily and intraday.

Garcia (2013) conducts a larger study analyzing the effect of sentiment on asset prices from 1905 to 2005. As a proxy for sentiment, they use the fraction of positive and negative words in specific columns of the financial news from the New York Times. They demonstrate that, even after accounting for other established time-series patterns, the predictability of stock returns based on news content is primarily concentrated during recessions. Specifically, a one standard deviation shift in news sentiment during recessions predicts a 12 basis point change in the conditional average return on the Dow Jones Industrial Average over one day, compared to only 3.5 basis points during expansions. This asymmetric predictability persists particularly on Mondays and post-holiday trading days, suggesting that investor sentiment significantly influences stock returns during adverse market conditions.

Arslan-Ayaydin, Boudt, and Thewissen (2016) study earnings releases press using a dictionary approach with two categories, positive and negative, and constructing a score from them. The study finds that managers with equity-based incentives often use a more positive tone in these releases to influence stock prices. By analyzing over 26,000 press releases from S&P 1500 firms between Q4 2004 and Q4 2012. They show that this optimistic tone increases with the proportion of managers' compensation tied to stock prices. However, the research also indicates that investors react less to these positive tones when they know managers have significant equity incentives, as they expect potential self-serving behavior and thus discount the stock's perceived value.

Calomiris and Mamaysky (2019) develops an approach to analyzing news through word flow measures (textual data acquired through consistent sources through time), including sentiment, frequency, unusualness (entropy), and topical context, applied to 51 countries from 1998 to 2015. They begin with the selection and preprocessing of a text corpus, which, for emerging markets (EMs), includes 5 million unique articles found in the Thomson Reuters database. For developed markets (DMs), the corpus comprises articles about countries identified as developed market economies. To weigh the relevance of word flow, they group words into topical clusters using the Louvain clustering method (which I detail later). The study identifies five topic clusters for EMs and DMs, with four clusters common to both countries. Then, entropy is defined by the probability distribution of 4-grams. Thus, articles are considered unusual if they contain language not commonly seen in the past. Additionally, sentiment analysis uses a dictionary-based approach with positive and negative words. The study divides the sample period into two parts, before and after February 2007, to account for changes during the global financial crisis. The findings demonstrate that word flow measures (sentiment, frequency, and entropy) can predict one-year ahead returns and drawdowns, capturing "collective unconscious" aspects of news that influence market behavior. These measures have greater predictive power for EMs but also significantly enhance forecasts for DMs.The study concludes that when contextualized (weighted) by topic and time, sentiment, frequency, and entropy measures can effectively forecast equity market risk and return.

Hassan, Hollander, van Lent, and Tahoun (2019) analyze the share of political discussions in quarterly earnings conference calls. They collect 178,173 conference calls from 7,357 firms listed in the United States between 2002 and 2016 from Thomson Reuters' StreetEvents. From

them, they create a firm-level measure of political risk. The methodology involves a dictionary approach to distinguish political from non-political language. They use training libraries of political and non-political texts to identify political bigrams, which are then counted in conference calls alongside terms related to risk and uncertainty. This generates a measure of the share of conversation about political risks. They validate this measure by accurately identifying political risk discussions and their intuitive variations over time and sectors. The measure correlates with firm actions and stock volatility, suggesting higher political risk leads to reduced hiring and investment and increased political lobbying and donations. The measure is robust to controls for political sentiment, ensuring it captures genuine political risk rather than general sentiment about political issues. The researchers also construct measures for non-political and overall risk, demonstrating the distinctiveness of their political risk measure.

Sautner, van Lent, Vilkov, and Zhang (2023) also used a dictionary-based approach to develop scores related to climate risk. However, they innovate by obtaining the list of words and n-grams using a keyword discovery algorithm proposed by King, Lam, and Roberts (2017). Their climate exposure measures capture the proportion of earnings calls related to climate change topics and are available for a global sample of over 10,000 firms in over 34 countries from 2002 to 2020. They demonstrate that these measures are helpful in predicting important real outcomes related to the net-zero transition, such as green tech growth and patenting. Additionally, they find that the measures contain information reflected in the options and equity markets.

2.2.2 NLP for financial documents

Feldman, Govindaraj, Livnat, and Segal (2010) examines whether non-financial information in the MD&A (Management's Discussion and Analysis) section of SEC filings (10-Q and 10-K) from 1993 to 2006 is linked to short-term and longer-term excess market returns. The study uses the frequency of positive and negative words in the MD&A sections as a crude indicator of the non-financial information's tone, comparing it to previous MD&A filings from the same firm. They find that shifts in the frequency of positive and negative words correlate significantly with short-term market returns around the time of SEC filings. These tone changes are also significantly correlated with longer-term drift excess returns, even after accounting for additionally disclosed financial information. The results suggest that market participants consider non-financial information in MD&A disclosures, supporting the SEC's requirement for these disclosures.

Jegadeesh and Wu (2013) introduces a new return-based term weighting scheme using positive and negative dictionaries. Considering 45,860 10-Ks filed from January 1995 through December 2010, grouping 7,606 unique firms, they observe that the scheme effectively measures document tone and shows a significant relationship with market returns around firms' 10-K filing dates. Unlike existing measures, it correlates with market reactions even when only positive word lists are used. By employing positive and negative word lexicons, the measure remains robust after controlling for various factors such as earnings announcement date returns, accruals, and volatility. Combining lexicons reduces subjectivity and demonstrates reliability even with incomplete or extraneous word lists. Additionally, the market's underreaction to the 10-K tone is

corrected within two weeks. The paper also applies the methodology's generalizability to initial public offering (IPO) prospectuses, finding a negative relationship between tone scores and IPO underpricing.

Bodnaruk, Loughran, and McDonald (2015) introduces a novel method for measuring firm-level financial constraints by analyzing the language used in 10-K disclosures filed with the SEC from 1996 to 2011. Unlike traditional measures that rely on macro-level firm characteristics, their approach focuses on the frequency of "constraining words" found in the text. this study employs the percentage of constraining words in the 10-K text as a primary indicator of financial constraint, identifying 184 specific words such as "required" or "obligations". The paper argues that this linguistic approach offers advantages over traditional methods, particularly in identifying inflection points where firms may become financially constrained. The research tests the ability of the percentage of constraining words to predict liquidity events, such as dividend omissions or increases, equity recycling, and underfunded pensions. Their results suggest that this linguistic measure outperforms widely used financial constraint indexes in predicting these events, even after controlling for standard firm characteristics.

2.2.3 Vector representation of paragraphs

Le and Mikolov (2014) introduced the Paragraph Vector (doc2vec) model, which extends word vectors to sentences, paragraphs, and documents, capturing semantic meaning in fixed-length vectors through neural network training. Lau and Baldwin (2016) empirically evaluated doc2vec, highlighting its performance variability depending on hyperparameters and data, and provided practical insights for effective empirical use. Adosoglou, Lombardo, and Pardalos (2021) used doc2vec to analyze 10-Ks from 1998 to 2018, comparing them with traditional methods, such as dictionary-based ones, to capture changes linked to future abnormal returns. The study introduced a Semantic Similarity Portfolio (SSP) strategy, finding that firms with minimal semantic changes in their 10-Ks, particularly those with a year-on-year doc2vec cosine similarity above 0.95 and positive previous year returns, tend to achieve significant future risk-adjusted abnormal returns, up to 10% annually. Despite the promising results, their approach is limited by the computational time required for model training and the need to account for executive changes.

2.2.4 Topic clustering

To group articles by topics and weight their relevance to infer markets Calomiris and Mamaysky (2019) (presented earlier), attempt to find significant topics using the Louvain method. By constructing a vector of occurrences of words for each article (effectively associating vector to document) and defining a score of similarity between them, they can form a network of similarities. The unsupervised Louvain method is then applied to find relevant sub-network clusters of articles they define as topics.

Curiskis, Drake, Osborn, and Kennedy (2020) compared the performance of various document clustering and topic modeling methods on social media text data. They highlighted that document and word embeddings, particularly doc2vec, are effective for document clustering, outperforming

traditional tf-idf approaches and other topic modeling techniques. Specifically, doc2vec embeddings combined with k-means clustering yielded the best results. They demonstrated two significant outcomes for clustering with doc2vec embeddings on data segmented by document length. First, the optimal number of training epochs decreases as the document character length increases. Second, doc2vec embeddings with k-means clustering consistently performed well across different document lengths.

2.3 Cyber risk and expected returns of stocks

Jamilov, Rey, and Tahoun (2023) build a dictionary-based measure of cyber risk exposure using quarterly earnings calls of more than 13,000 firms from 85 countries over 2002-2021. Their dictionary of cyber-related words was qualitatively validated using the predictability of realized cyberattacks. The paper also provides evidence that the cyber risk measure is valid and reflects economically meaningful firm-level variation in cyber risk. The paper presents case studies of cyberattacked and cybersecurity firms, as well as snippets from actual call transcripts of select firms. It shows that the measures can predict reported cyberattacks in the subsequent one, four, and eight quarters. Additionally, the paper demonstrates that the measures are associated with stock market outcomes and realized volatility and validates the measures against 10-K files. The paper also provides a global description of cyber risk exposure, as the data used contains firms from 85 countries and documents shifting geographical patterns. To explain the geography of cyber risk, the paper extends the canonical gravity model with proxies of financial, legal, and geopolitical proximity to the U.S. The paper finds that U.S. equity portfolio holdings in destination countries robustly predict cyber exposure. The paper also presents the dynamics of cyber exposure across sectors and characterizes firms as more likely to be cyberattacked. The paper also shows that cyber risk uncertainty is priced in the options market and that market-based protection costs against price, variance, and downside risks are greater for firms with higher cyber risk exposure. The paper argues that cyber risk exposure at present times signals future potential stock market or real economic deterioration.

Florackis, Louca, Michaely, and Weber (2023) present a new firm-level measure of cybersecurity risk, which is derived from the textual analysis of cybersecurity risk disclosures in the "Item 1A Risk Factors" section of 10-K statements from 2007 to 2018. To build their measure for a given firm at a given time, they compare section 1A of the firm of interest to section 1A from previously known cyber-attacked firms. The comparison is done by transforming all text sections into vectors of word occurrences and applying cosine similarities to compare them. The authors find that this dictionary-based measure effectively identifies firms that extensively discuss cybersecurity risk. The measure also exhibits plausible time-series and cross-sectional characteristics, such as a positive trend over time and a higher prevalence among industries heavily relying on information technology. They also find the measure correlates with characteristics such as size, age, growth opportunities, asset tangibility, R&D expenditures, and trade secrets. Furthermore, they find that the measure predicts the probability of a firm experiencing a future cyberattack. The paper also examines the relationship between cybersecurity risk and stock returns, finding that

a portfolio that goes long on stocks with high cybersecurity risk and short on stocks with low cybersecurity risk earns a statistically significant return premium of 66-69 basis points per month, or up to 8.3% per year, in equal-weighted returns. This result is robust to various specifications and subsamples. Fama-MacBeth cross-sectional regressions confirm a positive and statistically significant association between future stock returns and their cybersecurity risk measure. The authors also find that a cybersecurity-based portfolio performs poorly around heightened investor attention to cybersecurity risk but earns a high premium during other times. They also conduct an out-of-sample test that exploits the large-scale hack of SolarWinds, finding that firms with higher ex-ante cybersecurity risk scores, according to their measure, exhibit negative cumulative abnormal returns around the hack.

Celeny and Maréchal (2023) present a novel method for estimating firms cyber risk using doc2vec trained on MITRE ATT&CK cybersecurity knowledgebase and applied on 10-K statements.[1] This method outperforms traditional dictionary-based approaches by considering the whole 10-K statement instead of specific sections and capturing broader contextual information. The resulting cyber risk score is uncorrelated with other firm characteristics. They show that a portfolio of U.S.-listed stocks in the high cyber risk quintile achieves an excess return of 18.72% annually. Additionally, a long-short portfolio based on these cyber risk scores shows a significant positive risk premium of 6.93% annually. The study establishes that cyber risk is a critical factor in pricing the cross-section of stock returns, as confirmed by their Bayesian asset pricing method. Their analysis also reveals that portfolios sorted by cyber risk score exhibit a positive and statistically significant alpha over traditional factor models, with an average monthly excess return of 0.56%. Furthermore, they show qualitatively that sorting firms with other risk factors such as market beta, firm size, and book-to-market value, then sorting those firms by their cyber risk to build a portfolio leaves invariant that a high cyber risk portfolio performs better than low ones. Cyber risk-based portfolio also carries a significant premium in Fama-Macbeth regressions. Their proposed method outperforms a similar approach by Florackis et al. (2023), achieving superior results using doc2vec instead of a dictionary-based approach and the previous 10-K as textual references. This approach avoids problems like classifying firms as zero-risk and does not require historical cyberattack data, providing a more accurate measure of latent cyber risk. Robustness tests confirm the method's reliability, showing that the cyber risk factor remains consistent over time and is unaffected by the exclusion of cybersecurity firms from the sample.

Liu, Marsh, and Xiao (2022) analyze how firms' sensitivities to cybercrime impact the pricing of individual stocks and equity portfolios, utilizing a news-based cybercrime index and corroborating findings with Google search trends data. The index is calculated by counting all cybercrime-related news references scaled by the total news references. It is based on newly published content from approximately 40,000 internet news sites from 1998 to 2021. They confirm that a significant negative correlation between cybercrime exposures and subsequent stock returns exists, using bivariate portfolio-level analyses and stock-level cross-sectional regressions using well-known pric-

[1] Available at https://attack.mitre.org/

ing factors. The study highlights the importance of cybercrime sensitivity as a key factor in asset pricing. It provides insights into how firm-specific factors such as corporate governance, industry dynamics, digitization, and IT investments influence a firm's vulnerability to cyber threats. Finally, they show that high cybercrime beta stocks significantly outperform low beta stocks across 112 significant cyber incidents affecting the U.S. economy.

Gomes, Mihet, and Risbabh (2023) use different regression methods to link various sets of firm-specific financial and innovation-based variables to cyber risk, cyber security, and cyber innovation. Creating the variables involved counting patents related and unrelated to cyber security and using the cyber risk score developed by Florackis et al. (2023) to determine to which extent a firm is cyber risky. They show that the threat of cybercrime drives innovation in cybersecurity measures, which fosters technological advancements and long-term growth, particularly in digitally savvy firms that develop these measures in-house. Those firms protect themselves against cyber risks and enhance the quality of their other digital products. The study also finds that firms in states with early data breach notification laws show the strongest response to cyber risks, suggesting that the severity and costs of cybercrime have escalated, impacting firms' ability to invest in innovation. They also introduce a growth model in the context of cyber security and innovation. The model indicates that digitally-savvy firms benefit from in-house cybersecurity, while non-digitally-savvy firms rely on less tailored, external cybersecurity solutions.

Hypotheses

H1. The cyber risk of financial documents is unique

- H1.a There is no structure (clusters) in the various MITRE ATT&CK tactics
- H1.b When firm returns are sorted by different types of cyber risk, there is no significant over/underperformance.

H2. The tone/sentiment of paragraphs related to cybersecurity has no influence

Chapter 3

Data

3.1 Market data

I download public equity data from Wharton Research Data Services[2] (WRDS), and their API. The data originated from the Center for Research in Security Prices[3] (CRSP) and S&P Global Market Intelligence's Compustat database[4]. I report the list of variables in Table A.1 and Table 3.1 report their statistics after cleaning.

I use a pre-existing Python script that retrieves all available data from WRDS about various firms and filters out those that have not filed 10-K forms with the SEC. I extract monthly stock returns and financial ratios for 7,079 firms between January 2007 and December 2023. I depict the industry distribution of these firms using the Fama-French 12 industry distribution in Figure 3.1.

I also download the one-month Treasury bill rate and returns on the market, book-to-market (HML), size (SMB), momentum (UMD), investment (CMA), and operating profitability (RMW) factors from the Kenneth French data repository[5].

[2] https://wrds-www.wharton.upenn.edu/
[3] https://crsp.org/
[4] https://www.marketplace.spglobal.com/en/datasets/compustat-financials-(8)
[5] http://mba.tuck.dartmouth.edu/pages/faculty/ken.french/data_library.html

Variable	Mean	Std	Min	Max	P1	P25	P50	P75	P99
firm size	20.17	2.49	13.11	26.33	13.68	18.54	20.33	21.87	25.66
firm age	2.42	1.15	-2.48	4.13	-1.39	1.83	2.67	3.24	4.05
ROA	-0.15	0.54	-4.30	0.49	-3.04	-0.13	0.02	0.06	0.37
book to market	0.73	1.19	0.00	99.55	0.02	0.26	0.50	0.86	4.56
TobinQ	2.11	2.14	0.35	24.15	0.56	1.03	1.39	2.24	11.80
MktBeta	1.15	0.87	-3.00	5.91	-1.15	0.65	1.08	1.55	3.99
intangibles to assets	0.15	0.21	0.00	8.10	0.00	0.00	0.05	0.24	0.78
debt to assets	0.57	0.30	0.03	1.81	0.05	0.34	0.55	0.78	1.48
ROE	-0.08	0.61	-5.88	1.60	-2.96	-0.07	0.07	0.15	0.87
price to earnings	-0.87	132.55	-2001.73	455.35	-568.94	-3.93	12.05	22.64	295.69
profit margin	-0.42	6.46	-111.45	1.00	-27.21	0.22	0.39	0.62	0.96
asset turnover	0.82	0.74	0.00	4.09	0.01	0.25	0.66	1.16	3.42
cash ratio	2.07	3.89	0.01	36.13	0.01	0.23	0.68	1.98	20.28
sales to invested cap	1.39	1.50	0.00	10.42	0.01	0.44	0.94	1.77	8.13
capital ratio	0.31	0.32	-0.10	1.97	0.00	0.03	0.24	0.47	1.51
RD to sales	0.75	5.08	0.00	89.34	0.00	0.00	0.00	0.06	22.67
ROCE	-0.00	0.44	-3.21	1.30	-1.98	-0.01	0.09	0.17	0.93
readability	16.08	1.07	7.14	19.89	13.19	15.51	16.31	16.81	18.08
secret (dummy)	0.28	0.45	0.00	1.00	0.00	0.00	0.00	1.00	1.00
risk length table	5.03	1.46	0.00	7.69	0.00	4.84	5.35	5.81	6.84
volume per cap	0.28	6.52	-1.91	3485.03	-0.01	0.06	0.13	0.23	1.97
humans per capital $\times 10^6$	8.40	157.41	0.00	16689.97	0.00	0.50	1.50	4.19	71.49
humans per assets $\times 10^6$	4.29	14.04	0.00	879.49	0.00	0.38	1.75	4.08	42.02

Table 3.1: **Descriptive statistics of the firm characteristics**

This table provides descriptive statistics for various firm characteristics from 2009 to 2023. Mean, standard deviation (Std), minimum (Min), and maximum (Max) values are reported. Percentiles (P1, P25, P50, P75, P99) are also included. Firm-level characteristics are winsorized at the 1st and 99th percentile (by year). The characteristics are defined in Table A.1

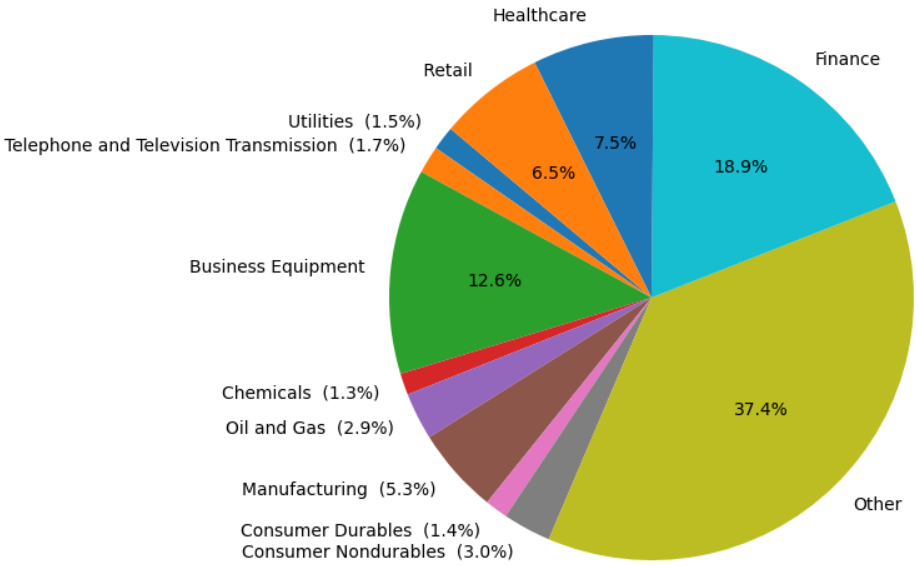

Figure 3.1: **Industry distribution**

Distribution of firms in the 12 Fama-French industries. Standard Industrial Classification (SIC) codes are obtained from CRSP. The conversion table, from SIC to 12 FamaFrench industries, is available on the Kenneth French data repository.

3.2 10-K statements

10-K statements are financial filings publicly traded companies submit annually to the U.S. Securities and Exchange Commission (SEC). They contain information such as companies' financial statements, risk factors, and executive compensation. 10-K statements will later be used to build a cybersecurity risk measure. The index files from the SEC's Edgar archives[6] are used to download and structure the 10-K. These index files contain information about all the documents filed by all firms for a specific quarter. Each line of the index file corresponds to a 10-K and is structured as follows:

CIK | Company Name | Form Type | Date Filed | Filename

Where Filename is the URL under which an HTML version of the document is available. Their Central Index Key (CIK) is used to identify firms. The CIK consists of a number used by the SEC to identify corporations and individuals who have filed disclosures. I use a Python script that goes through these index files and identifies URLs corresponding to 10-K statements using the Form Type entry. These URLs are matched to one of the 7,079 firms using the CIK entry. 64,988 10-K statements are identified, corresponding to 2.73 statements per firm on average. The evolution of the number of 10-K filled annually is reported in Figure 3.2.

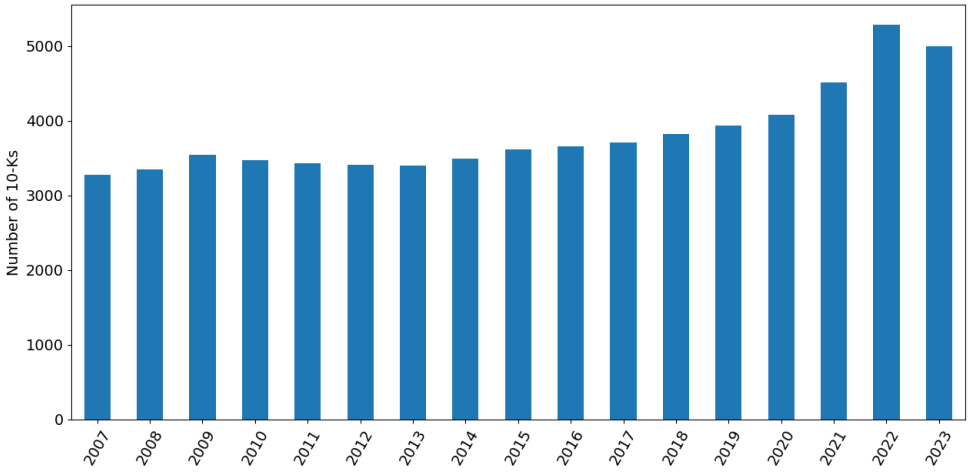

Figure 3.2: **Number of 10-Ks per year**

Number of companies in the study sample that have filed a 10-K statement through the years.

3.3 MITRE ATT&CK description

The MITRE ATT&CK[7] cybersecurity knowledge base is used as a reference for cyber attack descriptions. This knowledge base was created in 2013 to document cyber attack tactics, techniques, and procedures. It is structured by tactics, techniques, and sub-techniques as depicted in Figure 3.3. There are 14 tactics: reconnaissance, resource development, initial access, execution,

[6] https://www.sec.gov/Archives/edgar/full-index/
[7] https://attack.mitre.org/

persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, command and control, exfiltration, and impact. There are 785 sub-techniques across all tactics. Two examples of sub-techniques are given in Table 3.2.

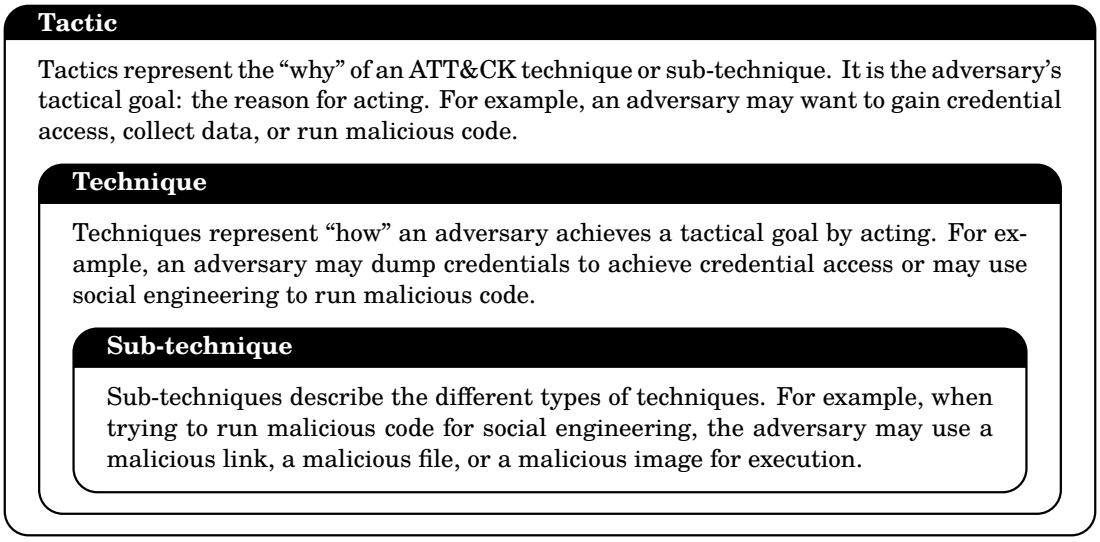

Figure 3.3: **Structure of MITRE ATT&CK**

		Description
Tactic	Credential Access	Adversaries may forge web cookies that can be used to gain access to web applications or Internet services. Web applications and services (hosted in cloud SaaS environments or on-premise servers) often use session cookies to authenticate and authorize user access.
Technique	Forge Web Credentials	
Sub-technique	Web Cookies	
Tactic	Reconnaissance	Adversaries may gather employee names that can be used during targeting. Employee names can be used to derive email addresses as well as to help guide other reconnaissance efforts and/or craft more believable lures.
Technique	Gather Victim Identity Information	
Sub-technique	Employee Names	

Table 3.2: **Examples of sub-techniques from MITRE ATT&CK**

Figure 3.3 and Table 3.2 are taken from Celeny and Maréchal (2023). The Data section closely follows their approach, and much of their code has been repurposed to suit my requirements. The additional data primarily originates from 2023.

Chapter 4

Methodology

4.1 Cyber score

To compute the cyber scores of interest, I start with the 14 individual MITRE ATT&CK tactics: Reconnaissance, Resource, Development, Initial Access Execution, Persistence, Privilege Escalation, Defense Evasion, Credential, Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact. To reduce this dimensionality, I aggregate them with clustering methods (see 4.1.4) that yield the following "supertactics": Command and data manipulation, Credential movement, Persistence and evasion, Preparation and reconnaissance. For comparison, I also add the overall score, aggregating all 14 categories into one, corresponding to the score obtained in Celeny and Maréchal (2023). Finally, I add a variation of the overall score that relates better to the risk notion: the cyber sentiment score.

4.1.1 pre-processing

Everything related to text processing and its use is done exactly as described in Celeny and Maréchal (2023). I download 10-K statements from the SEC Archives as HTML files. Then, I use the library BeautifulSoup to extract usable texts from HTML.[8] I remove punctuation and numbers and set all letters to lowercase. Finally, I apply the Python script of Celeny and Maréchal (2023) that uses the "wordfreq" and NLTK libraries to divide the text into sentences, remove stop-words such as "the", "is", "and", ...) and remove the most common words.[9][10]

After pre-processing, the average length of the MITRE ATT&CK sub-technique descriptions is 39.7 words. I use a Python algorithm to merge consecutive sentences from 10-K statements into paragraphs with an average length of close to 40 words after pre-processing. This results in an average of 640 paragraphs per 10-K statement with 46 words per paragraph. The standard deviation is 2.8 words per paragraph and 309 paragraphs per 10-K statement.

[8] https://www.crummy.com/software/BeautifulSoup/
[9] https://pypi.org/project/wordfreq/
[10] https://www.nltk.org/

4.1.2 Paragraph Vector algorithm (doc2vec)

As in Celeny and Maréchal (2023), I use the paragraph to vector model proposed by Le and Mikolov (2014), which is an extension of the word2vec model (Mikolov, Chen, Corrado, and Dean, 2013). There are various advantages to working with this NLP approach compared to others, such as the dictionary approach. First, the comprehension of the method is semantical, meaning that it is not limited to a count of word frequencies. The word order impacts the resulting vector, and paragraphs with similar or synonym words will have close vector representations. Second, training the model with specific text that involves a particular vocabulary allows the incorporation of relatively unknown words. Finally, the resulting vectors have a dimension usually much smaller than vectors resulting from the dictionary approach.

Two versions of the model exist, the distributed memory model (DM) and the distributed bag-of-words model (DBOW). In the DM, a neural network is trained as follows. First, a word is removed in a paragraph. Then, inputting the paragraph vector representation and context words (also in vector representation) surrounding the missing word, the neural network is optimized by trying to guess the missing word. In the DBOW, the neural network is trained to predict a series of words sampled from a paragraph using only the vector representation of the paragraph as input. Figure 4.1 illustrates the training process of the two models.

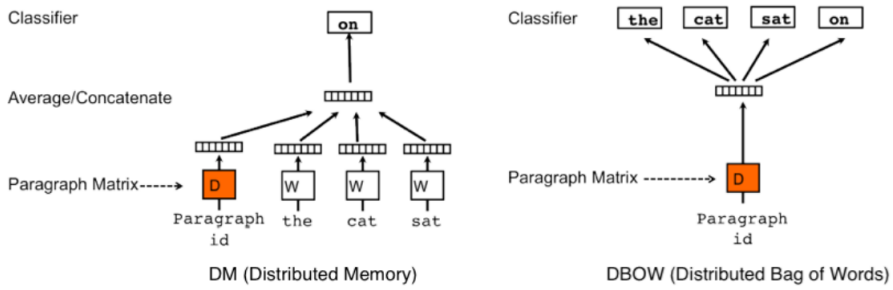

Figure 4.1: **Illustration of doc2vec training**

Illustration of the training of the neural network of the two versions of doc2vec, distributed memory model (DM) and distributed bag-of-words model (DBOW). The figure is taken from Le and Mikolov (2014).

The training data and details, the hyperparameters and their validation, and the final model choice are extensively covered in Celeny and Maréchal (2023). This work uses their saved doc2vec model.[11]

4.1.3 Cosine similarity

Using the doc2vec method previously described, all paragraphs of interest can be embedded into vectors. A common way to attribute a similarity score to two paragraph vectors is to take the cosine of the angle they form. Other ways exist, but only measuring the angle was proven more effective than considering the vectors' magnitude (see Adosoglou et al., 2021). This is because

[11] https://github.com/technometrics-lab/17-Cyber-risk_and_the_cross-section_of_stock_returns

the latter is more affected by the random initialization of weights during training in the neural network that outputs the vectors.

4.1.4 Cyber tactics clustering

I disentangle the overall cyber score obtained in Celeny and Maréchal (2023). The idea is that the risk coming from different areas of cyber security might not be similarly priced and, therefore, should not be aggregated into a single score but rather be separated into sub-cyber scores. A natural way of splitting the overall score into different categories comes from the written structure of MITRE ATT&CK, with 14 categories already mentioned in chapter 4.1. However, it is believed that splitting the overall score to such an extent might result in a loss of explanatory power and highly correlated sub-cyber scores. Therefore, aggregating the 14 tactics into a few super tactics might mitigate the negative effect of splitting the overall score.

On the other hand, with the doc2vec method and the similarity score, I can transform every 785 sub-techniques (paragraphs) of MITRE ATT&CK into vectors and compare their similarity. This process results in a similarity matrix of dimension 785 by 785, onto which clustering methods can be applied. Indeed, the similarity matrix can be understood as the representation of a network where every 785 nodes (paragraphs) are connected by edge values weighted by their similarity. In this context, I present three classical clustering methods.

The first and most simplistic clustering method is K-Means. Note that since the input similarity matrix is based on cosine similarity, it is rather designated as spherical K-Means, where the distance between each point to class into K categories is understood as the angle between the vectors defined by those points rather than the Euclidian distance between those points. Either version of K-Means works as follows: It begins by randomly setting initial cluster centroids, then iteratively assigns each data point (paragraphs) to the nearest centroid and updates the centroids by recalculating their mean positions among their associated data points. The process is repeated until convergence. Note that although the K-Means algorithm always converges, it is relatively dependent on the initial centroid guess. The user must choose the number of clusters K without prior knowledge. The algorithm generally produces rough results but often reveals an initial simple structure in the similarity of the provided data.

The second method is much more powerful as it requires no prior hyperparameters; thus, the number of clusters is an output of the method. The Louvain method, explained in Blondel, Guillaume, Lambiotte, and Lefebvre (2008), provides a straightforward way to identify clusters (groups of nodes within a graph that are more densely connected) in a network. To explain the Louvain method, I first need to introduce the notion of modularity. It is defined as a value in the range $[-1/2, 1]$ that measures the density of links within communities compared to links between communities. For a weighted graph, modularity is defined as:

$$Q = \frac{1}{2m} \sum_{i=1}^{N} \sum_{j=1}^{N} \left[S_{ij} - \frac{k_i k_j}{2m} \right] \delta(c_i, c_j),$$

where S_{ij} represents the edge weight between nodes i and j, in this case, this is the similarity

matrix. k_i and k_j are the sum of the weights of the edges attached to nodes i and j, respectively. m is the sum of all the graph's edge weights. N is the total number of nodes in the graph. c_i and c_j are the communities to which the nodes i and j belong and δ is the Kronecker delta function. The Louvain method works as follows. Initially, each node is assigned to its own community. Then, the method iterates through two phases: the first phase optimizes modularity locally by moving individual nodes between communities to maximize the increase in modularity. The second phase aggregates the nodes in each community in the first phase into single nodes and builds a new network, where the communities found in the first phase are treated as nodes. Phases one and two are repeated until no further improvement in modularity is possible. The final partitioning of nodes into communities is returned as a result.

The third clustering method is spherical K-means on a dimensionally reduced similarity matrix. The spectral clustering method works as follows. First, the degree matrix D is constructed. it consists in a diagonal matrix where each entry D_{ii} represents the sum of similarities for node i and is computed as $D_{ii} = \sum_j S_{ij}$. The Laplacian matrix L is defined as $L = D - S$. The spectral clustering algorithm computes the eigenvectors and eigenvalues of the Laplacian matrix L. Let $\lambda_1, \lambda_2, ..., \lambda_N$ be the eigenvalues and $v_1, v_2, ..., v_N$ be the corresponding eigenvectors. After obtaining the eigenvectors, I select the K eigenvectors corresponding to the K smallest eigenvalues (excluding the smallest eigenvalue, typically zero). I arrange these eigenvectors as columns in a matrix V of dimension K by N. Finally, I perform clustering on the rows of the matrix V using the k-means clustering method. The power of this approach is that I can choose the number of features necessary to perform a satisfying clustering (reducing from N=785 to K<20, for example, can radically improve the clustering by getting rid of superfluous dimensions).

Finally, a form of scoring is needed to find the best clustering output produced by the wide range of hyperparameters and method choices. In this paper, I propose a rather simple but efficient approach that requires initial labelalization of each node. Each paragraph (node) is a sub-technique belonging to one of the 14 tactics of MITRE ATT&CK. Thus, they naturally already belong exclusively to 14 sub-clusters. The discrimination of clustering methods works on the following two requirements.

First, I want the paragraphs belonging to one tactic (sub-cluster) to belong to the same super-tactic, *i.e.*, the same cluster found by the method. Indeed, the paragraphs are initially classed by the creator of MITRE ATT&CK together because they share common characteristics. It would not be very sensible to spread them across different super-tactics (clusters) once the clustering method is applied. Thus, a measure of sub-cluster heterogeneity among clusters is needed. I use Shannon entropy, defined as follows:

$$H_{sub_j} = -\sum_{i=1}^{nb.clusters} P(sub_j)_i \log P(sub_j)_i \tag{4.1}$$

Where $P(sub_j)_i$ is the proportion of paragraphs of sub-cluster (tactic) j belonging to cluster (super tactic) i. Intuitively, if we are in an ideal case and the paragraphs of a sub-cluster j are entirely contained in cluster 1 we would have $P(sub_j)_1 = 1$ and $P(sub_j)_i = 0$ for $i \neq 1$, thus leading to

$H_{sub_j} = 0$ being minimal (mind the minus sign in the equation and the logarithm on number lower than 1). If we start to spread the paragraph of the sub-cluster among other clusters, the $P(sub_j)_i$ becomes different from 0 and 1, and H_{sub_j} gradually increases. To reduce the 14 H_{sub_j} to one score of discrimination, I sum them all, thus obtaining the Entropy sum, the measure of sub-cluster heterogeneity among clusters. The heterogeneity is high when the Entropy sum is low.

Second, I need a score to counter the following extreme case. All sub-clusters, but one may be classed into one cluster and the last sub-cluster into a second cluster. This would lead to a minimum Entropy sum of 0 but would have no value for my application. I want the sub-cluster to be reasonably spread out among the clusters. To translate this idea into a meaningful score, I create the Balanced score, defined as the standard deviation of the label counts. In other words, the clustering method produced an ordered list of 785 values corresponding to the label of the cluster each paragraph belongs to. For each label, I count the number of occurrences on the list. If the paragraphs are relatively well spread out across the cluster, then taking the standard deviation of all the count of the labels should be low since each cluster would contain approximately the same number of paragraphs. The last case to worry about is that the balanced score could be low, but the paragraph would be randomly spread across the cluster, thus not reflecting the initial structure of MITRE ATT&CK tactics (sub-clusters). To counter that, it is sufficient to consider the Entropy sum.

Considering the method that outputs the lowest Entropy sum and the lowest balanced score, I can effectively discriminate the different clustering methods' outputs. Note that there is no guideline regarding the optimal trade-off between the two scores, *i.e.* what additional amount is optimal to forfeit to the Entropy sum to lower the Balanced score and inversely.

Finally, the whole clustering process described here must be seen more as a guideline tool. Indeed, after choosing the best method, I class each paragraph in the cluster where most of its sub-cluster belongs, regardless of the method's output for the misplaced paragraphs. The structure of MITRE ATT&CK is probably more coherent than the output of any unsupervised clustering method. However, it is still advantageous to consider the new clustering structure output since it is based on the cosine similarity matrix, and it could maximize the likelihood of reducing the correlation between the different sub-cyber scores that will also be based on cosine similarities.

4.1.5 Setting the cyber score

At this point, each paragraph of a 10-K can be transformed into a vector, and the same can be done with the 785 paragraphs of MITRE ATT&CK. Then, each paragraph of the 10-K can be compared to each paragraph of MITRE ATT&CK. This leads to each paragraph of the 10-K being associated with 785 cosine similarities. Celeny and Maréchal (2023) computes the cyber score of a 10-K by associating the maximum out of the 785 cosine similarities to each paragraph and then taking the average of the top 99% of these maxima.

Similarly, I define a sub-cyber score by associating to each paragraph the cosine similarities of a subset of paragraphs of MITRE ATT&CK. For example each paragraph would be associated

to 120 cosine similarities (instead of 785) where 120 would correspond to the 120 paragraphs of MITRE ATT&CK that belongs to the same category (cluster or sub-cluster/ super tactic or tactic). Then the process of finding the sub-cyber score associated with a super tactic or tactic would be the same as described in the previous paragraph, I take the maximum out of the 120 cosine similarities for each paragraph and then compute the average of the top 99% of these maxima.

4.1.6 Sentiment analysis

To establish a cyber sentiment score, I opted for a simple approach. I define the cyber score as it was done in Celeny and Maréchal (2023), but instead of taking the maximum, I take 0 if the paragraph does not contain a word from a specific list and the maximum as usual if it does contain a word from the specific list.

The specific list is defined in Hassan et al. (2019) and is reported in the annex. It contains words relative to “risk” or “uncertainty” and was originally created using the Oxford English Dictionary.

4.2 Asset pricing tests

4.2.1 Univariate sorts

Five portfolios are constructed based on a cyber score of interest. Firms are classified each quarter based on their most recent known cyber score from the previous quarter. These firms are then divided into five categories corresponding to the quintiles of their cyber scores. Consequently, the firms in the top 20% of cyber scores are placed in Portfolio 5 (P5). After that, each firm is weighted within its portfolio according to its market capitalization known from the end of the previous quarter. The cyber-based portfolios are updated quarterly.

A first quantitative test consists of observing whether the average returns of each portfolio change monotonically with the increasing cyber score. The idea is to see if returns are affected by this cyber classification, thus hinting at a potential cyber-related risk structure.

Next, I assess the portfolio’s returns, controlling for pricing factors. By using pricing factors recognized in the literature (factors included in the CAPM, in Fama and French, 1992 (FFC) and in Fama and French, 2015 (FF5)), I observe if their linear combinations are sufficient to explain the returns of the portfolio or if statistically significant alpha (intercept) appear, meaning that the profitability of the portfolios based on cyber score can not be entirely explained by common pricing factor and new ones are needed.

4.2.2 Double sorts

The interest in the double sorting method is the same as in univariate sorting, I want to see if returns are affected by the cyber classification. However, the cyber score may be a proxy *i.e.* something that mimics another firm characteristic, such as the size, the book-to-market ratio, or

market beta. To avoid that, I sort the firms according to one of the three characteristics mentioned. These firms are then divided into five categories corresponding to the quintiles of their characteristic. Consequently, the firms in the top 20% of the characteristic of interest (for example, firms with the highest book-to-market ratio) are placed in category 5 (Q5). Then, for the firm of each category Q1 to Q5, I construct a portfolio based on a cyber score as described previously to obtain 25 portfolios, five for each category.

4.2.3 Cross-sectional tests

Fama and MacBeth (1973) proposes the following method. First, estimate betas using time series regressions with 2-year rolling windows (24 months). This corresponds to the following regression for each asset i with $t \in [T-24, T]$:

$$R_{i,t} = \alpha_{i,t} + \sum_k \beta_{i,T}^k F_{k,t} + \epsilon_{i,t}, \quad \forall i \tag{4.2}$$

Each asset returns R_i is regressed on pricing factors F_k non-proper to the firm (in my case, the FF5 factors are non-proper to the firm; they are not a characteristic of the firm; they should be included. On the contrary, the cyberscore is proper to the firm, so it should not be included). Consequently, I obtain time series of betas specific to both asset and factor: $\{\beta_i^k\}_{T=01/2009,\ldots,12/2023}$ (ranging from January 2009 to December 2023, in this example). Then, I build twenty portfolios based on the cyber score analogously to the five cyber score-based portfolios described earlier. Knowing the weight $x_{i,p,T}$ of each asset inside each portfolio through time, I can compute the factor exposures of the portfolios:

$$\beta_{p,T}^k = \sum_{i=1}^{20} x_{i,p,T} \cdot \beta_{i,T}^k \tag{4.3}$$

After that, the risk premia (gamma) are computed for each time t with $p = 1, \ldots, 20$:

$$R_{p,t} = \gamma_t^0 + \sum_k \gamma_t^k \beta_{p,t-1}^k + \sum_j c_t^j \lambda_{p,t-1}^j + \epsilon_{p,t}^*, \quad \forall t \tag{4.4}$$

Consequently, to determine each $\{\gamma_t^k\}_{t=01/2009,\ldots,12/2023}$, 20 portfolio returns are used each time in the linear regression. The additional terms are aggregated firm-specific factors. In my case, I only have one such factor (so j is omitted in the following expression), the cyber score:

$$\lambda_{p,t} = \sum_{i=1}^{20} x_{i,p,t} \cdot \lambda_{i,t} \tag{4.5}$$

The remaining coefficient $\{c_t\}_{t=01/2009,\ldots,12/2023}$ is determined alongside $\{\gamma_t^k\}_{t=01/2009,\ldots,12/2023}$ during the linear regression. Finally, a t-test is applied on each time series $\{\gamma_t^k, c_t\}_{t=01/2009,\ldots,12/2023}$ to assess the statistical significance of each risk premia.

4.2.4 Time-series tests

Gibbons et al. (1989) introduces a statistical test to assess portfolio pricing efficiency:

$$R_{i,t} = \alpha_i + \sum_p \beta_{i,p} R_{p,t} + \epsilon_{i,t}, \quad \forall i, \tag{4.6}$$

where $R_{i,t}$ and $R_{p,t}$ are assets and portfolio returns, respectively. If the portfolios were carefully selected, they could correctly predict the asset returns, thus suppressing the need for alphas (intercepts that contain contributions to their asset returns not taken into account by the explanatory portfolios). GRS provides a statistical test for this null hypothesis: H_0: $\alpha_i = 0 \quad \forall i$. Cochrane (2005) generalize this idea by including traded factors F_k instead as explanatory variables and portfolio excess returns as the endogenous one:

$$R^e_{p,t} = \alpha_p + \sum_k \beta_{p,k} F_{k,t} + \epsilon_{p,t} \tag{4.7}$$

In that case, the GRS score that tests jointly the zero alphas follows a F-distribution:

$$\frac{(T-N-K)}{N} \frac{\hat{\alpha}' \hat{\Sigma}^{-1} \hat{\alpha}}{1 + \hat{\mu}' \hat{\Omega}^{-1} \hat{\mu}} \sim F_{N,T-N-K}, \tag{4.8}$$

where T is the number of time periods, N is the number of portfolios, K is the number of factors, $\hat{\Sigma}$ is the residual covariance matrix, $\hat{\alpha}$ is the vector of alphas, $\hat{\mu}$ is the vector of average factor returns and $\hat{\Omega}$ is the covariance matrix of factors. Note that both $\hat{\Sigma}$ and $\hat{\Omega}$ must be estimated with the maximum likelihood estimator (biased version). The tests will be performed four times on four series of 20 portfolios constructed according to the cyber score, the size, the book-to-market ratio, and the market beta of involved firms.

4.2.5 Bayesian approach

Barillas and Shanken (2018) introduces three methods to test pricing factors. The first method is close to the GRS and commonly tests zero alpha for pricing factors and portfolio returns. The second method tests, for a given set of factors, if a subset of those factors is sufficient to price portfolio returns. The third method, on which I focus here, allows us to find which subset of factors, among a large given set of factors, are the best pricing factors. It is a "relative" method, meaning that no returns are required for the test. To produce the test, they first introduce the marginal likelihood associated with a given subset of factors:

$$\text{ML} = \text{ML}_U(f|Mkt) \cdot \text{ML}_R(f^*|Mkt, f) \cdot \text{ML}_R(r|Mkt, f, f^*) \tag{4.9}$$

Where f are the factors of the subset, f^* are the factors excluded from the subset (but in the general set), and Mkt is the market excess returns. Note that the third term can be ignored; it will later be canceled out since it is common to any subset of factors. $\text{ML}_U(Y|X)$ and $\text{ML}_R(Y|X)$ are based on the equations $Y_{t,n} = \alpha_n + X_t \beta_n + \epsilon_{t,n}$ and $Y_{t,n} = X_t \beta_n + \epsilon_{t,n}$. They can be computed

as follows:[12]

$$\mathbf{ML}_U(Y|X) = \left|X'X\right|^{-\frac{N}{2}} |S|^{-\frac{T-K}{2}} Q \tag{4.10}$$

$$\mathbf{ML}_R(Y|X) = \left|X'X\right|^{-\frac{N}{2}} |S_R|^{-\frac{T-K}{2}} \tag{4.11}$$

where $|S| = |\epsilon'\epsilon|$ and $|S_R| = |\epsilon'\epsilon|$ are the determinants of the N × N cross-product matrices of associated OLS residuals (R stand for restricted since $\alpha_n = 0$ is imposed on the second linear equation), T is the number of periods, K the number of factors in the regression (number of columns in X), and N the number of endogenous variable on the RHS of the linear equations (number of columns in Y). For example, $\mathbf{ML}_U(f^*|Mkt, f)$ could be associated with $[f^*_{1,t}, f^*_{2,t}] = [\alpha_1, \alpha_2] + [Mkt_t, f_{3,t}, f_{4,t}]\beta + [\epsilon^*_{1,t}, \epsilon^*_{2,t}]$ with $N = 2$, $K = 3$ and β a 3×2 matrix and the general set containing four factors $[f_1, f_2, f_3, f_4]$ (two included, two excluded marked by * in this example). The scalar Q is given by:

$$Q = \left(1 + \frac{a}{a+k}\left(\frac{W}{T}\right)\right)^{-\frac{T-K}{2}} \left(1 + \frac{k}{a}\right)^{-\frac{N}{2}} \tag{4.12}$$

$$a = \frac{1 + \hat{\mu}'\hat{\Omega}^{-1}\hat{\mu}}{T} \tag{4.13}$$

$$k = \frac{\hat{\mu}'\hat{\Omega}^{-1}\hat{\mu}}{N}(1 - \text{prior}^2) \tag{4.14}$$

$$W = T\frac{\hat{\alpha}'\hat{\Sigma}^{-1}\hat{\alpha}}{1 + \hat{\mu}'\hat{\Omega}^{-1}\hat{\mu}}, \tag{4.15}$$

where $\hat{\Sigma}$ is the residual covariance matrix, $\hat{\alpha}$ is the vector of alphas, $\hat{\mu}$ is the vector of average X factor, and $\hat{\Omega}$ is the covariance matrix of X factors. Note that both $\hat{\Sigma}$ and $\hat{\Omega}$ must be estimated with the maximum likelihood estimator (biased version). Finally, the prior is an arbitrary number. Barillas and Shanken (2018) use 1.25, 1.5, 2, and 3 in their empirical test. Intuitively, the prior help to set k, the expected increment to the squared Sharpe ratio $Sh(X)^2 = \hat{\mu}'\hat{\Omega}^{-1}\hat{\mu}$ from the addition of one more factor. Once the relevant marginal likelihoods are computed, the probability p_j associated with a subset of factors M_j being better pricing factors than other subsets is given by:

$$p_j = \frac{\mathbf{ML}_j \times P(M_j)}{\sum_i \mathbf{ML}_i \times P(M_i)}, \tag{4.16}$$

where $\mathbf{ML}_j$ is the marginal likelihood associated with the subset M_j and $P(M_j)$ is the prior probability of the subset M_j. In general, Barillas and Shanken (2018) advise all prior probabilities to be constant and equal since there is no particular reason to favor a specific subset of factors. Note that the third term in Eq. 4.9 cancels at this last step.

Following this methodology in Barillas and Shanken (2018), p_j can be computed with subsets, including the cyber score as a factor and others without, to compare its pricing ability.

---

[12] $\overset{(T\times N)}{Y} = \overset{(1\times N)}{\alpha} + \overset{(T\times K)(K\times N)}{X\quad\beta} + \overset{(T\times N)}{\epsilon}$, note that α has not the correct dimension here, it is to reflect the fact that α is constant across t for a given n.

Chapter 5

Results

5.1 Clustering of MITRE ATT&CK

I apply the clustering methods on the cosine similarity matrix created from MITRE ATT&CK paragraphs vector embeddings. This allows for identifying the relevant sub-cyber score tied to previously mentioned super tactics (command and data manipulation, credential movement, persistence and evasion, and preparation and reconnaissance). I report the results of various attempts with different clustering methods in Figures 5.1, 5.2, and 5.3. The K-means methods provide a coherent but crude initial structure that I report in Figure 5.1. Indeed, the paragraphs tend to be well spread across the super tactics (clusters) but at the cost of heterogeneity, with the exclusivity of a tactic in a super tactic being inexistent. This results in a low balanced score at the cost of entropy, as depicted in Figure 5.4.

Figure 5.2 shows the performance of the Louvain method. This method greatly improves the heterogeneity, especially with tactics 5 and 12 (resource development and reconnaissance) being exclusive to cluster 1 (the super tactic: preparation and reconnaissance). However, not putting a threshold on the inputted similarity matrix component induces the Louvain method to create two superfluous clusters. Hence, I include those restrictions. Indeed, when comparing two paragraphs of MITRE ATT&CK, it is not uncommon to encounter sentences with similar structures for different semantic content. Thus, I tone down the similarity of a highly too similar paragraph with a higher threshold. Conversely, I define a lower threshold such that similarities that are too low and, therefore, most likely noise that reflects no similarity are set to zero.

The last method can be seen as a safeguard for the output of the Louvain method. Applying the spectral clustering method, I retrieve the structure previously encountered with higher heterogeneity than with K-means. If the hyperparameters are correctly tuned, the output is similar to the Louvain method's, particularly for $n = 4$ and $egn = 6$. I report the results in Figure 5.3. Including more dimensions (higher egn value) adds noise and decreases the clustering quality.

Finally, I select the output of the Louvain method as a baseline to group the tactics without splitting them across super tactics. Although Figure 5.4 shows that outputs of other methods may be slightly better, I favor the Louvain method since no additional hyperparameters tuning is required.

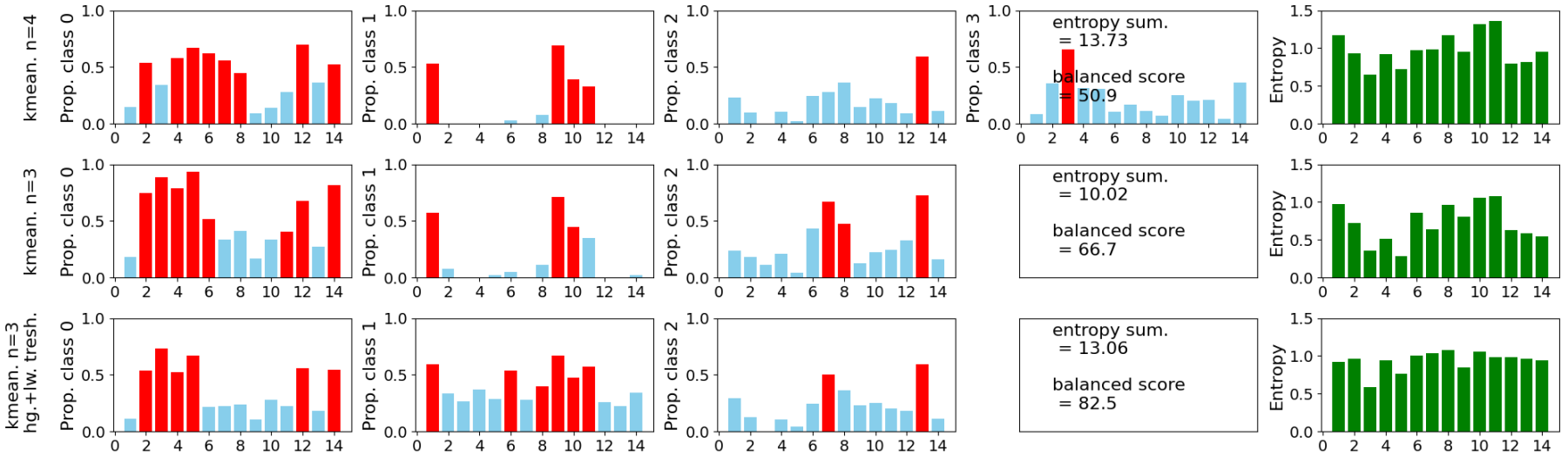

Figure 5.1: **Clustering results part.1**

This figure presents the results of each clustering method indicated on the left. The figure in red and blue represents $P(sub_j)_i$, the proportion of paragraphs of sub-cluster (tactic) j belonging to cluster (super tactic) i. The 14 sub-cluster labels are on the x-axis of each figure, and the cluster labels correspond to the columns (class 0 to 3, here). If the proportion is in red, it means it is the highest in the cluster (in other clusters/columns, the same sub-cluster will be in blue). I also report the entropy sum and the balanced score on the figure for each method. Finally, the individual Shannon entropy of each sub-cluster is reported in green in the last column. In the name of the method, I also indicate the hyperparameters of the method. Here, n corresponds to the number of clusters imposed by the k-means method. "hg. tresh." and "lw. tresh." corresponds to a change applied to the similarity matrix. If the value in the similarity matrix is lower than 0.25, it is changed to 0 (lower threshold), and if the similarity is higher than 0.85, it is changed to 0.5 (higher threshold). In part.2 and part.3 "egn" corresponds to the K eigenvectors in the spectral clustering. I also made the output clusters of each method match. Hence, the comparison is simpler (otherwise, what the Louvain method called cluster 2 is not necessarily cluster 2 for the k-means method). The following list shows the corresponding number of each tactic : 1: Persistence, 2: Command and Control, 3: Impact, 4: Initial Access, 5: Resource Development, 6: Collection, 7: Exfiltration, 8: Credential Access, 9: Privilege Escalation, 10: Execution, 11: Defense Evasion, 12: Reconnaissance, 13: Lateral Movement, 14: Discovery.

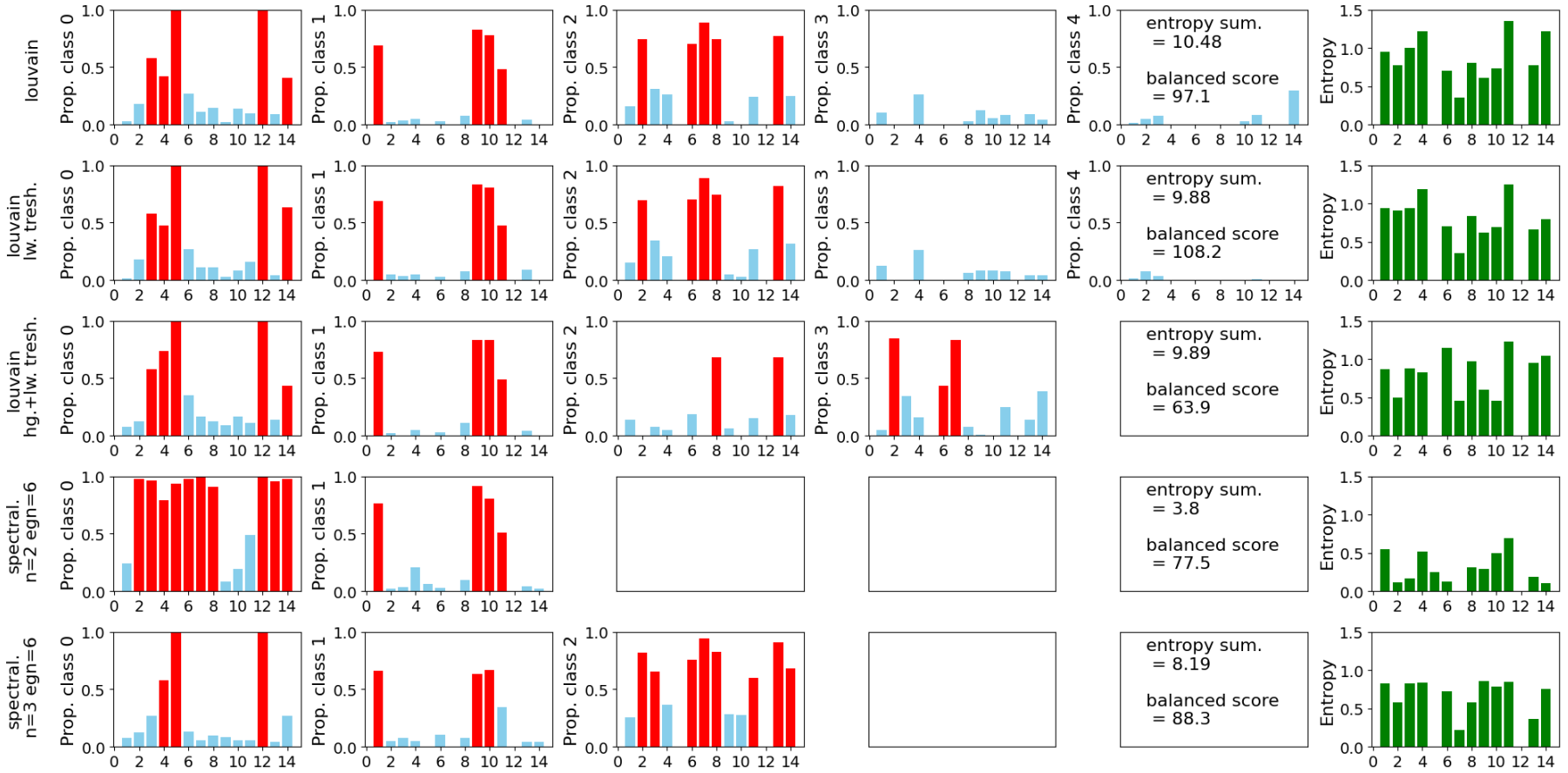

Figure 5.2: **Clustering results part.2**

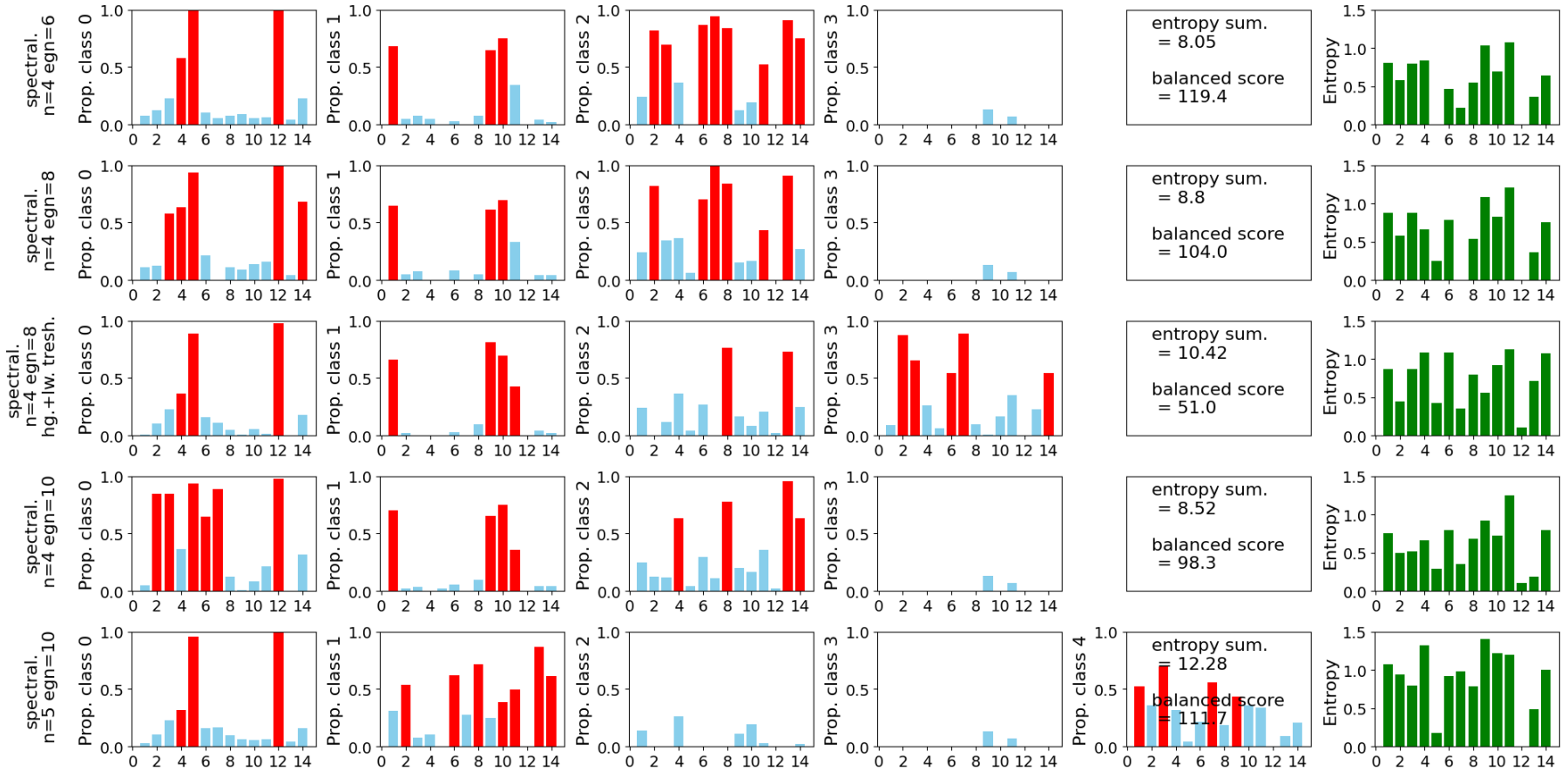

Figure 5.3: **Clustering results part.3**

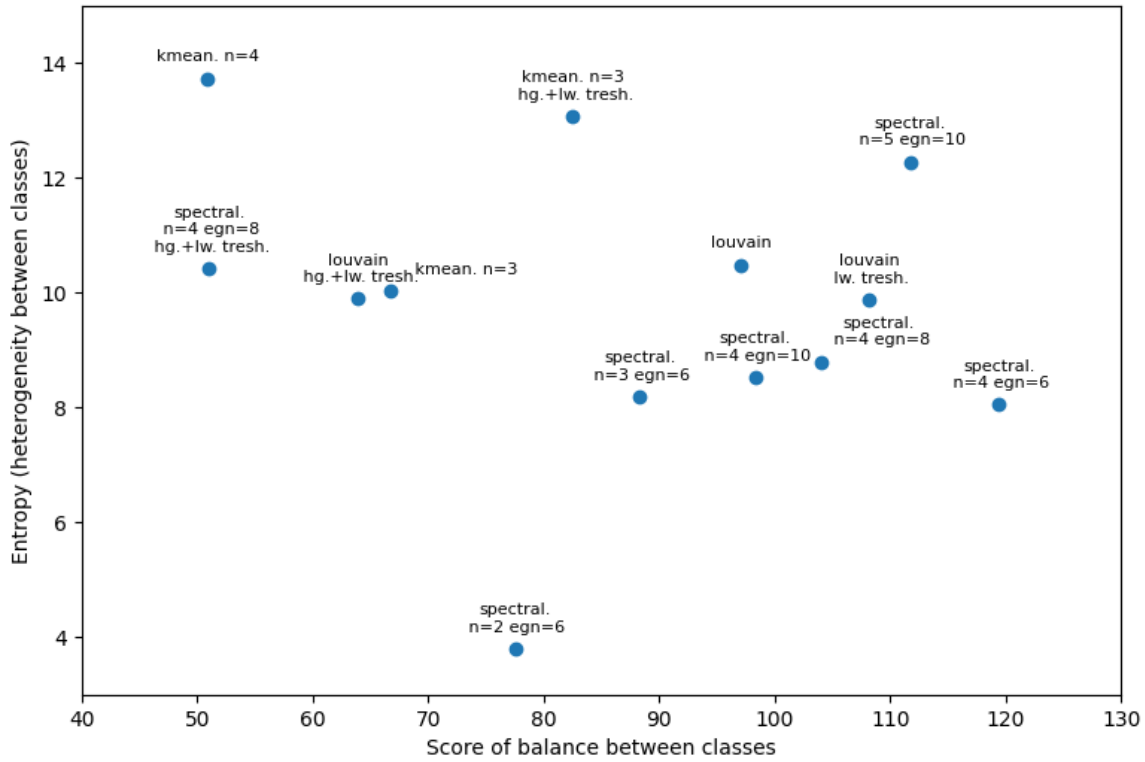

Figure 5.4: **Comparison of clustering scores: Entropy sum and Balanced score**

Each clustering method of Figure 5.1, 5.2, and 5.3 is presented here using their respective entropy sum and balanced score. Recall that the aim was to reduce both scores to distinguish the best clustering method. Also, note that there is no guideline regarding what additional amount is optimal to forfeit to the entropy sum to lower the balanced score and inversely.

This yields the following cluster/super tactics. I named each of them after their content:

Preparation and Reconnaissance: This super tactic encompasses tactics that adversaries use to prepare and gather information before launching an attack. **Impact** involves actions that disrupt, destroy, or manipulate systems and data to achieve the attacker's objectives. **Initial Access** includes techniques that adversaries use to gain an initial foothold within a network, such as exploiting vulnerabilities or using spear phishing. **Resource Development** entails the acquisition of resources like infrastructure, tools, and credentials necessary to support operations. **Reconnaissance** involves gathering information about the target environment to identify potential entry points and vulnerabilities. **Discovery** refers to techniques used to explore and map the target environment, such as network scanning and enumeration.

Persistence and Evasion: Once inside a target network, adversaries employ these tactics to maintain their foothold and avoid detection. **Persistence** ensures the attacker can maintain access even if the system is rebooted or credentials are changed, through techniques like installing malware or creating rogue accounts. **Privilege Escalation** involves gaining higher-level permissions to access more sensitive information and critical systems. **Execution** refers to running malicious code on a victim system, often necessary to carry out the attacker's objectives. **Defense**

Evasion includes a variety of methods to avoid detection and thwart defensive measures, such as disabling security software, obfuscating code, or using fileless malware.

Credential Movement: This group focuses on techniques used to steal and use credentials to move within a network. **Credential Access** involves obtaining account names, passwords, and other secrets that allow attackers to authenticate themselves as legitimate users. Techniques include keylogging, credential dumping, and brute force attacks. **Lateral Movement** is the process of moving through a network to find and access additional targets or more valuable data. This can be done using remote services, exploiting trust relationships, or leveraging legitimate credentials to access other systems and resources.

Command and Data Manipulation: In this phase, adversaries exert control over compromised systems and manipulate data to achieve their goals. **Command and Control** involves establishing a communication channel with the compromised environment to issue commands and control malware. This can be achieved through techniques like using web traffic, DNS, or custom protocols to communicate with command servers. **Collection** refers to gathering sensitive information from compromised systems, such as capturing screenshots, logging keystrokes, or accessing stored files. **Exfiltration** involves transferring the collected data out of the target network to an external location controlled by the adversary, often using encrypted channels or covert methods to avoid detection.

5.2 Cyber scores statistical descriptions

From the identified super tactics, I construct the cyber scores from the 10-Ks of each firm through the years. Table 5.1 presents the statistics related to each cyber score (the 14 tactics of MITRE ATT&CK, the four super tactics, the overall score, and the cyber sentiment score). Although their distribution appears similar, several facts must be considered. First, the statistics are for the whole sample, but the distribution is time-varying as Figures 5.5, 5.6, 5.7, and 5.8 suggest. This means that cyber scores evolving at different rates could be misrepresented. Second, the cosine similarity implies, in theory, a distribution ranging from -1 to 1, whereas the scores are much more narrowly distributed empirically. Thus, the slight variation observed in Table 5.1 is more meaningful than simple noise.

Two additional aspects must also be reported. First, some tactics lose relevance in the 10-Ks over time, and evidence of the cyber scores reflecting cyber risk has yet to be presented. However, this first feature is encouraging since the cyber scores are evolving differently, showcasing a shift of cyber-related information in the 10-Ks. Second, the cyber sentiment score has a higher 99 percentile than the other score, implying that taking out non-risk-related scores effectively removes points previously belonging to the top one percentile.

	Mean	Std	Min	Max	P1	P25	P50	P75	P99
Persistence	0.49	0.03	0.27	0.64	0.44	0.47	0.49	0.51	0.58
Command and Control	0.47	0.03	0.28	0.62	0.42	0.45	0.47	0.49	0.55
Impact	0.47	0.03	0.25	0.59	0.41	0.45	0.47	0.50	0.55
Initial Access	0.46	0.03	0.23	0.59	0.40	0.44	0.46	0.48	0.55
Resource Development	0.47	0.03	0.23	0.62	0.41	0.44	0.47	0.49	0.56
Collection	0.49	0.03	0.29	0.64	0.43	0.46	0.48	0.51	0.57
Exfiltration	0.47	0.03	0.23	0.64	0.41	0.44	0.46	0.49	0.56
Credential Access	0.50	0.03	0.29	0.64	0.43	0.47	0.49	0.52	0.58
Privilege Escalation	0.48	0.03	0.27	0.64	0.43	0.46	0.47	0.49	0.56
Execution	0.46	0.03	0.29	0.61	0.42	0.44	0.46	0.48	0.55
Defense Evasion	0.51	0.03	0.29	0.65	0.46	0.49	0.50	0.52	0.59
Reconnaissance	0.48	0.03	0.32	0.61	0.42	0.46	0.48	0.51	0.57
Lateral Movement	0.47	0.03	0.26	0.64	0.43	0.45	0.47	0.49	0.56
Discovery	0.48	0.03	0.31	0.63	0.43	0.46	0.47	0.49	0.56
Preparation and Reconnaissance	0.50	0.03	0.33	0.64	0.44	0.48	0.50	0.53	0.58
Persistence and Evasion	0.51	0.03	0.29	0.65	0.46	0.49	0.51	0.53	0.59
Credential Movement	0.50	0.03	0.29	0.65	0.44	0.48	0.50	0.52	0.59
Command and Data Manipulation	0.50	0.03	0.29	0.64	0.44	0.47	0.49	0.52	0.58
Overall	0.53	0.03	0.33	0.65	0.47	0.50	0.52	0.54	0.61
Sentiment	0.51	0.05	0.00	0.72	0.42	0.48	0.51	0.54	0.63

Table 5.1: **Descriptive statistics of the firm characteristics**

This table provides descriptive statistics for the 14 MITRE ATT&CK tactics cyber score, the four aggregated sub-cyber scores of the super-tactics, the overall cyber score, and the cyber sentiment score. The statistics are computed from all firms from 2009 to 2023.

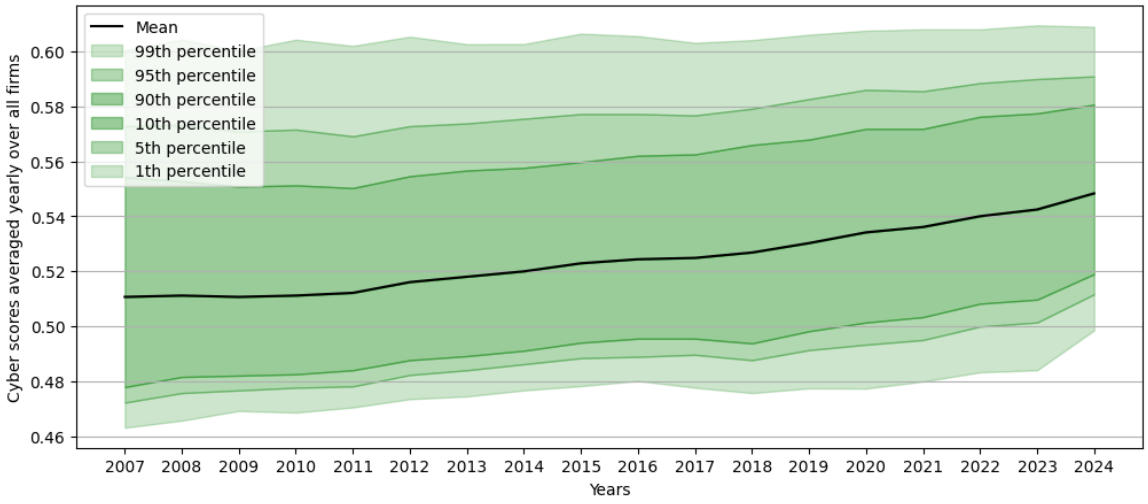

Figure 5.5: **Evolution of the overall cyber score averaged yearly over all firms**

The figure shows the evolution of the overall cyber score over all firms yearly. Each year provides a distribution of the cyber score over all firms that can be sorted to provide percentiles of interest and the averaged cyber score for a given year.

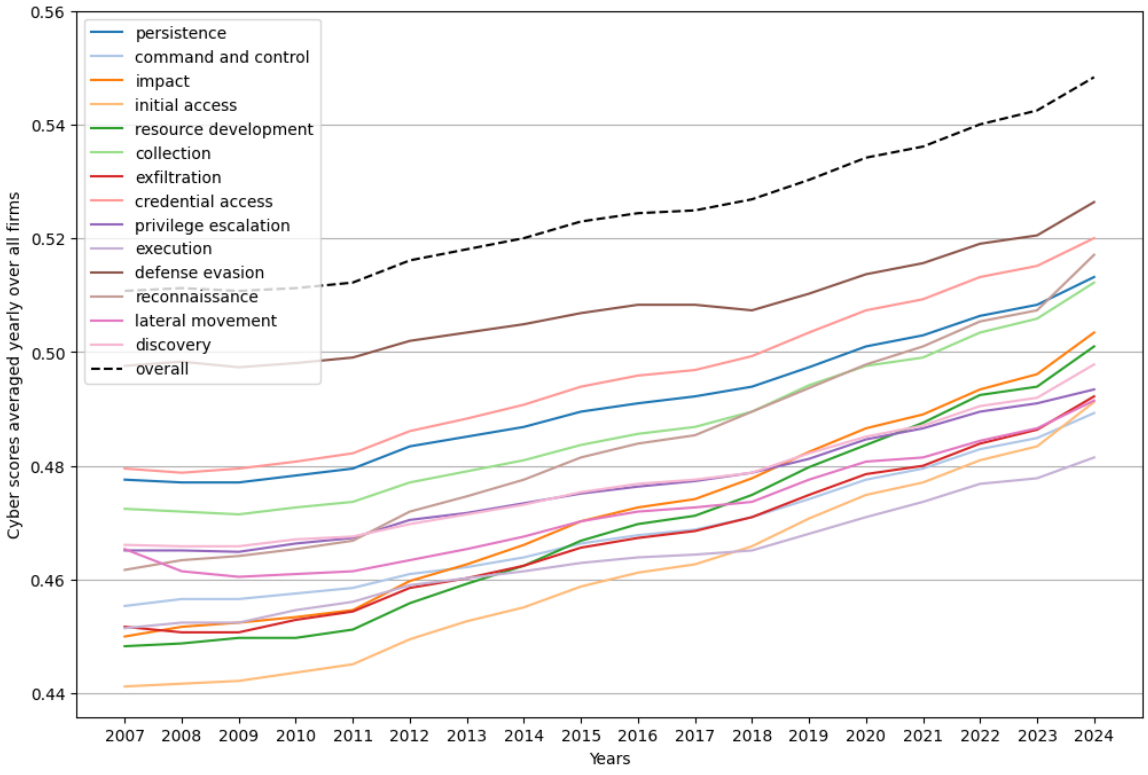

Figure 5.6: **Evolution of the sub-cyber scores related to the 14 tactics averaged yearly over all firms**

The figure shows the evolution of the 14 sub-cyber scores averaged over all firms yearly. The overall cyber score is also included to allow comparison.

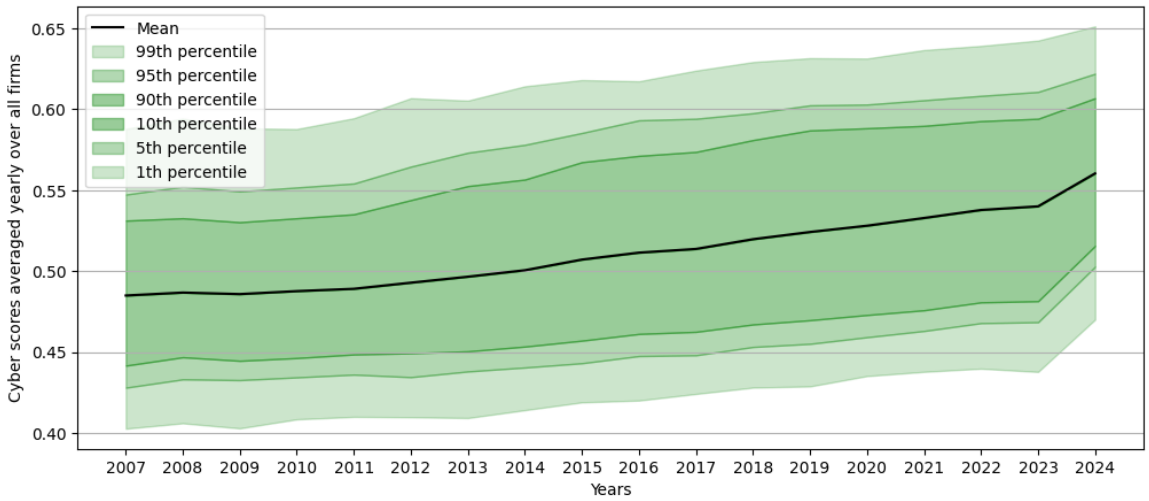

Figure 5.7: **Evolution of the cyber sentiment score averaged yearly over all firms**

The figure shows the evolution of the cyber sentiment score over all firms yearly. Each year provides a distribution of the cyber score over all firms that can be sorted to provide percentiles of interest and the averaged cyber score for a given year.

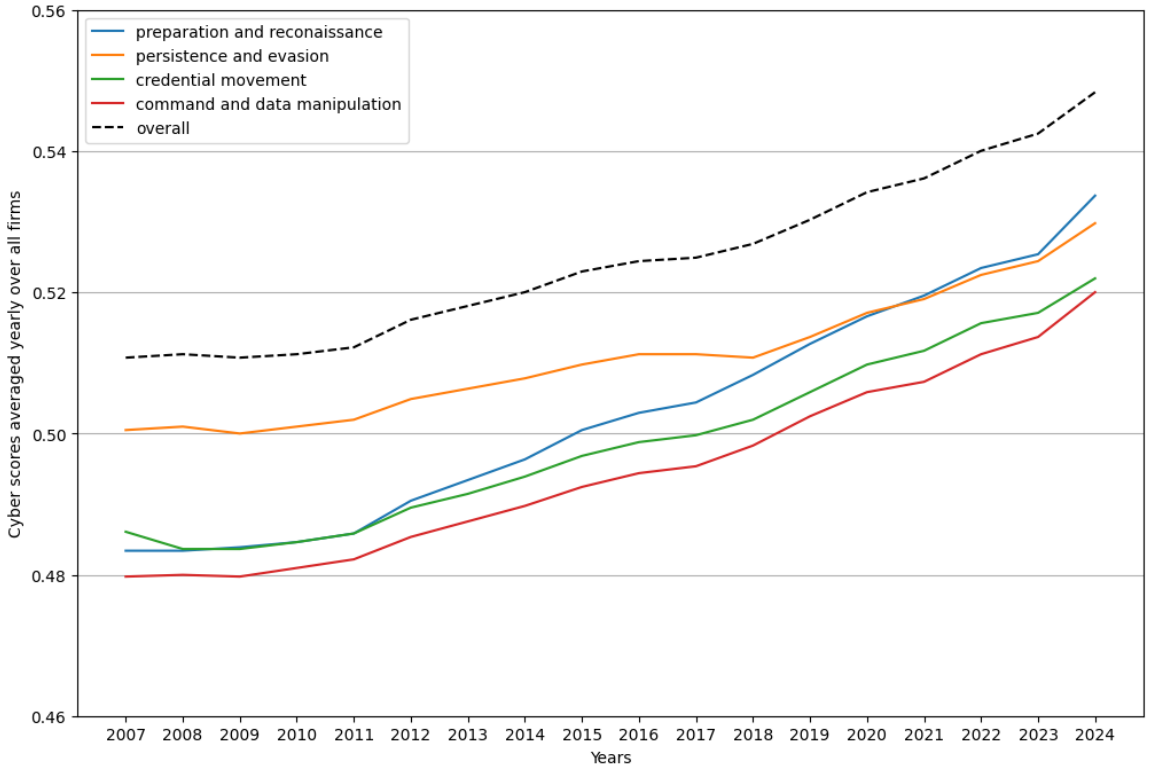

Figure 5.8: **Evolution of the sub-cyber scores related to the four super-tactics averaged yearly over all firms**

The figure shows the evolution of the four sub-cyber scores averaged over all firms yearly. The overall cyber score is also included to allow comparison.

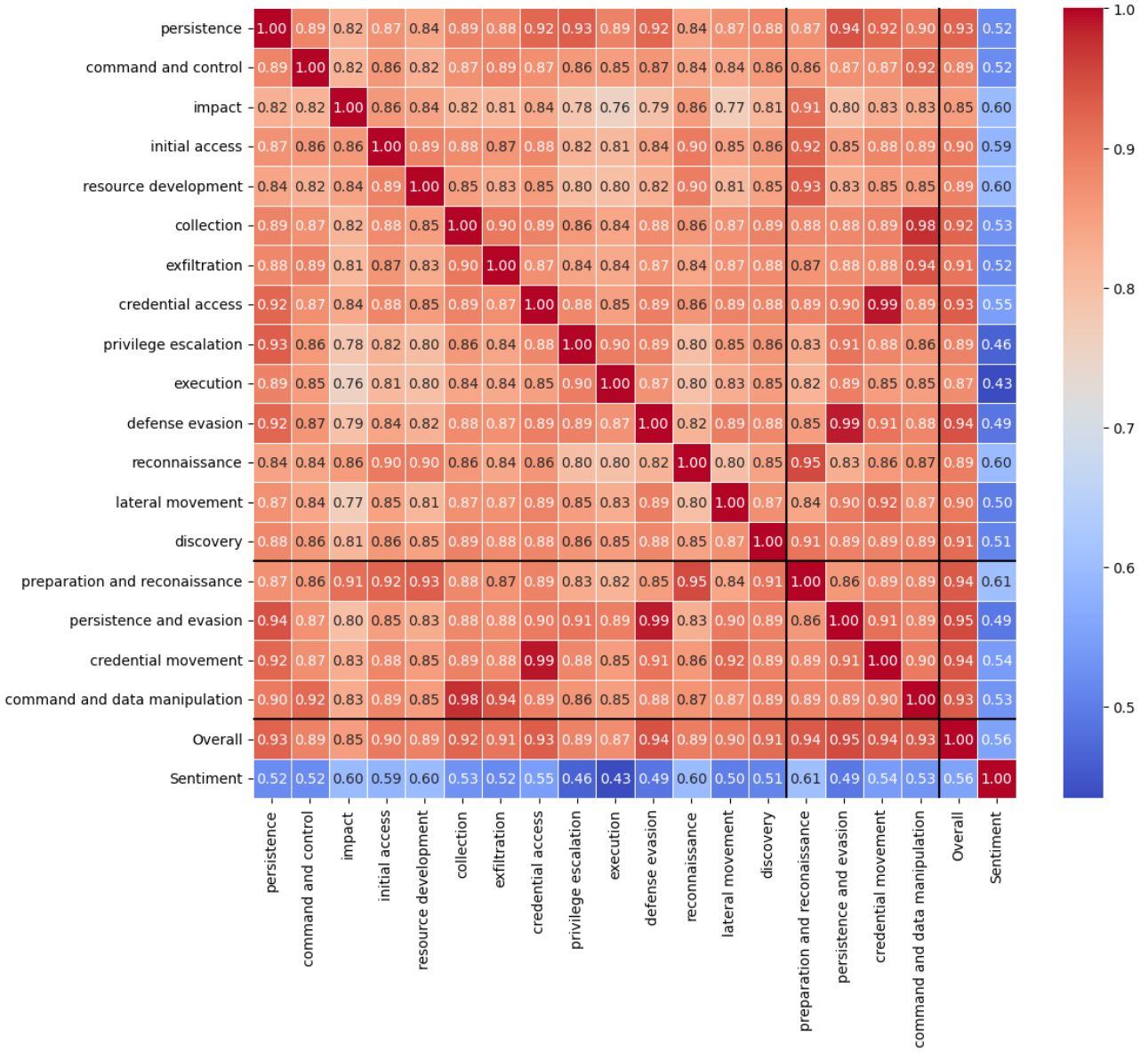

Figure 5.9: **Correlations of all cyber scores**

Firm-wise correlations of the sub-cyber scores of the 14 MITRE ATT&CK tactics, the 4 aggregated sub-cyber scores of the super-tactics, as well as the overall cyber score and the cyber sentiment score are presented here.

I present the correlation between cyber scores at the firm level (non-aggregated) in Figure 5.9. Unsurprisingly, the correlations between all scores are high, except for the sentiment score, which differs in its construction. This is expected since all scores come from the same doc2vec neural network output.

5.3 Cyber scores and financial characteristics

To ensure that the cyber scores are innovative and not the combination of other existent characteristics of the firm, I present the linear regression of the cyber scores of interest in Tables 5.2, 5.3, 5.4, 5.5, 5.6, and 5.7. Compared to Celeny and Maréchal (2023), I add the following variables: readability, secret, risk length table, volume per capital, and humans per capital. I describe all variables in Table A.1. The first three variables were part of the tested explanatory variables in Florackis et al. (2023). Including the risk length table shows the critical improvement made with the cyber score of this paper. Indeed, Florackis et al. (2023) report t-statistics of 40.80 and 20.59 for models 1 and 2, respectively. In my case, those t-statistics are significantly lower, improving my score's independence with non-semantic variables.

I include a new explanatory variable in the models with the following underlying idea: If there is a limited number of employees in a firm with highly valuable assets, those assets are more likely to be technological and could be cyber risky. This risk would then be reported in the 10-Ks and thus be reflected in the cyber score. This choice proves relevant as the Tables report t-statistics close to 10 for all cyber scores. The coefficient negative sign supports the view that the lower the human capital ratio, the higher it should be reflected on the cyber score. [13]

The statistical significance of other coefficients does not depart too much from the previous studies, with most of the variables being statistically non-significant or with the same sign as in Celeny and Maréchal (2023), especially at the firm level. Note that, despite adding new variables with higher t-statistics, the R^2 within is still low. It shows that additional variables cannot fully explain the different cyber scores. Furthermore, different t-statistics are obtained for each cyber score for the same coefficient. This suggests that each score could proxy for an intrinsically different risk for the firm.

Figure 5.10 displays the correlation of all cyber scores with the mentioned variables. As expected, variables with generally higher t-statistics tend to correlate more to the cyber scores. However, The correlation with "secret" must be taken cautiously since it is a dummy variable and the cyber score is close to 0.5; the correlation may be spurious or, at best, not informative.

Figure 5.11 shows the average cyber scores across industries. The overall score is always higher than other scores when controlling for industry. This was already the case in Table 5.1. The cyber sentiment score displays much fewer differences across industries when compared to other scores. This suggests that the score does not contain additional information or even destroy some of it at the industry level. As mentioned in Celeny and Maréchal (2023), industries that rely more heavily on technology, like Business Equipment or Telephone and Television Transmission, potentially report their cyber risk and thus have higher cyber scores. One can also observe that the different cyber scores vary differently across the industry, further highlighting the potential changes in the source of cyber risk disclosed in the 10-Ks.

[13] Additionally, I compute the covariance and correlation of each cyber score with the idiosyncratic volatility of firms. The results are presented in Appendix A.2. I thank Prof. Julien Hugonnier for this comment.

Dependent variable: Firm-level indicator of cyber score		
	Model 1	Model 2
Constant	**50.514*****	**53.229*****
	[46.66]	[65.46]
Firm Size (ln)	**0.008**	**0.039**
	[0.16]	[1.37]
Firm Age (ln)	**-0.346*****	**-0.492*****
	[-2.93]	[-8.80]
ROA	**0.027**	**0.014**
	[0.25]	[0.08]
Book to Market	**-0.028*****	**-0.138*****
	[-2.66]	[-5.04]
Tobin's Q	**0.026****	**0.158*****
	[2.55]	[7.73]
Market Beta	**-0.057***	**-0.115*****
	[-1.95]	[-2.83]
Intangibles/Assets	**-0.335***	**1.133*****
	[-1.75]	[5.51]
Debt/Assets	**-0.486****	**1.088*****
	[-2.13]	[2.59]
ROE	**-0.009**	**0.011**
	[-0.19]	[0.12]
Price/Earnings	**0.0003****	**0.00001**
	[2.10]	[0.04]
Profit Margin	**0.001**	**0.023*****
	[0.17]	[3.08]
Asset Turnover	**-0.056**	**-0.438*****
	[-0.66]	[-3.52]
Cash Ratio	**-0.0003**	**0.005**
	[-0.04]	[0.31]
Sales/Invested Capital	**0.013**	**0.134****
	[0.39]	[2.30]
Capital Ratio	**0.048**	**-2.200*****
	[0.25]	[-6.95]
R&D/Sales	**-0.005**	**-0.004**
	[-0.89]	[-0.42]
ROCE	**0.040**	**0.306***
	[0.43]	[1.92]
Readability	**0.090*****	**-0.164*****
	[2.81]	[-2.93]
Secret	**0.205***	**0.711*****
	[1.80]	[6.98]
Risk Length Table	**0.139*****	**0.254*****
	[4.67]	[7.36]
Volume per Cap.	**0.001**	**0.007*****
	[0.27]	[3.79]
Humans per Cap.	**-0.0004*****	**-0.000**
	[-11.02]	[-1.18]
Year fixed effect	Yes	Yes
Industry fixed effect	No	Yes
Firm fixed effect	Yes	No
Observations	25531	25531
R^2 within	0.3193	0.2672

Table 5.2: **Determinants of firm-level overall cyber score**

This table reports the results of cyber score regressions on firm characteristics. Year-, industry-, and firm-fixed effects are controlled. T-statistics are reported in brackets. The variables are standardized, and the standard errors are clustered at the firm level. $*$, $**$, and $***$ indicate significance at the 10%, 5% and 1% levels, respectively. All characteristics are defined in Table A.1.

Dependent variable: Firm-level indicator of cyber score		
	Model 1	Model 2
Constant	**43.921*****	**36.239*****
	[18.44]	[26.16]
Firm Size (ln)	**0.1046**	**0.2436*****
	[1.12]	[5.99]
Firm Age (ln)	**-0.6886*****	**-0.4258*****
	[-2.91]	[-5.15]
ROA	**-0.3729****	**-0.4243***
	[-2.07]	[-1.89]
Book to Market	**-0.0068**	**-0.0861****
	[-0.22]	[-2.07]
Market Beta	**-0.0759**	**0.0189**
	[-1.22]	[0.32]
Intangibles/Assets	**0.4**	**1.5571*****
	[1.02]	[5.33]
Debt/Assets	**0.1785**	**3.1032*****
	[0.37]	[5.77]
ROE	**-0.082**	**-0.0041**
	[-0.78]	[-0.03]
Price/Earnings	**-0.0002**	**-0.0003**
	[-0.89]	[-0.83]
Profit Margin	**-0.0059**	**0.0095**
	[-0.56]	[0.86]
Asset Turnover	**-0.0891**	**-0.1494**
	[-0.51]	[-0.8]
Cash Ratio	**0.0121**	**0.0217**
	[0.72]	[1.02]
Sales/Invested Capital	**-0.0733**	**-0.0916**
	[-1.14]	[-1.08]
Capital Ratio	**-0.12**	**-3.4501*****
	[-0.31]	[-8.31]
R&D/Sales	**-0.0225**	**-0.021**
	[-1.48]	[-1.48]
ROCE	**0.2894**	**0.4123***
	[1.47]	[1.74]
Readability	**0.1335**	**0.2959*****
	[1.1]	[2.85]
Secret	**0.4***	**0.5921*****
	[1.88]	[4.31]
Risk Length Table	**0.568*****	**0.7207*****
	[7.21]	[10.8]
Volume per Cap.	**-0.0044**	**-0.0029**
	[-0.9]	[-0.99]
Humans per Cap.	**-0.0014*****	**0.0005*****
	[-8.1]	[6.33]
Year fixed effect	Yes	Yes
Industry fixed effect	No	Yes
Firm fixed effect	Yes	No
Observations	25531	25531
R^2 within	0.2221	0.2088

Table 5.3: **Determinants of firm-level cyber sentiment score**

This table reports the results of cyber score regressions on firm characteristics. Year-, industry-, and firm-fixed effects are controlled. T-statistics are reported in brackets. The variables are standardized, and the standard errors are clustered at the firm level. $*$, $**$, and $***$ indicate significance at the 10%, 5% and 1% levels, respectively. All characteristics are defined in Table A.1.

Dependent variable: Firm-level indicator of cyber score		
	Model 1	Model 2
Constant	**48.709*****	**49.389*****
	[42.27]	[53.32]
Firm Size (ln)	**-0.014**	**0.0394**
	[-0.27]	[1.32]
Firm Age (ln)	**-0.5965*****	**-0.4996*****
	[-4.72]	[-8.04]
ROA	**0.0168**	**0.0293**
	[0.14]	[0.15]
Book to Market	**-0.0224****	**-0.1448*****
	[-1.97]	[-5.48]
Market Beta	**-0.0446**	**-0.1203*****
	[-1.45]	[-2.69]
Intangibles/Assets	**-0.3246**	**1.3698*****
	[-1.53]	[6.14]
Debt/Assets	**-0.626****	**0.8444***
	[-2.4]	[1.83]
ROE	**-0.0561**	**-0.0365**
	[-1.06]	[-0.39]
Price/Earnings	**0.0**	**-0.0003**
	[0.09]	[-0.96]
Profit Margin	**-0.0017**	**0.0259*****
	[-0.29]	[3.23]
Asset Turnover	**0.047**	**-0.5544*****
	[0.54]	[-4.03]
Cash Ratio	**0.0028**	**0.0129**
	[0.3]	[0.81]
Sales/Invested Capital	**-0.0259**	**0.1951*****
	[-0.7]	[3.06]
Capital Ratio	**0.1883**	**-2.2148*****
	[0.88]	[-6.28]
R&D/Sales	**-0.0063**	**0.0003**
	[-0.79]	[0.03]
ROCE	**0.097**	**0.3042***
	[0.93]	[1.73]
Readability	**0.0869****	**-0.1231****
	[2.47]	[-2.02]
Secret	**0.293****	**0.8431*****
	[2.47]	[7.77]
Risk Length Table	**0.118*****	**0.2876*****
	[3.6]	[6.68]
Volume per Cap.	**-0.0034**	**0.006*****
	[-1.05]	[2.66]
Humans per Cap.	**-0.0003*****	**-0.0001**
	[-9.34]	[-1.47]
Year fixed effect	Yes	Yes
Industry fixed effect	No	Yes
Firm fixed effect	Yes	No
Observations	25531	25531
R^2 within	0.3224	0.2677

Table 5.4: **Determinants of firm-level command and data manipulation cyber score**

This table reports the results of cyber score regressions on firm characteristics. Year-, industry-, and firm-fixed effects are controlled. T-statistics are reported in brackets. The variables are standardized, and the standard errors are clustered at the firm level. $*$, $**$, and $***$ indicate significance at the 10%, 5% and 1% levels, respectively. All characteristics are defined in Table A.1.

Dependent variable: Firm-level indicator of cyber score		
	Model 1	Model 2
Constant	**49.779*****	**50.925*****
	[41.1]	[57.92]
Firm Size (ln)	**-0.0834**	**-0.005**
	[-1.5]	[-0.16]
Firm Age (ln)	**-0.6247*****	**-0.5823*****
	[-4.97]	[-9.58]
ROA	**0.0446**	**0.0669**
	[0.4]	[0.34]
Book to Market	**-0.0085**	**-0.1247*****
	[-0.63]	[-3.88]
Market Beta	**-0.0529**	**-0.1494*****
	[-1.64]	[-3.4]
Intangibles/Assets	**-0.2478**	**1.0274*****
	[-1.2]	[4.62]
Debt/Assets	**-0.588****	**1.0181****
	[-2.33]	[2.29]
ROE	**0.008**	**0.0121**
	[0.15]	[0.13]
Price/Earnings	**0.0003***	**-0.0**
	[1.92]	[-0.04]
Profit Margin	**-0.0015**	**0.022*****
	[-0.26]	[2.97]
Asset Turnover	**-0.164***	**-0.5367*****
	[-1.83]	[-3.96]
Cash Ratio	**-0.0005**	**-0.0024**
	[-0.06]	[-0.15]
Sales/Invested Capital	**0.0404**	**0.1481****
	[1.17]	[2.42]
Capital Ratio	**0.2001**	**-2.1857*****
	[0.98]	[-6.42]
R&D/Sales	**-0.0093**	**-0.011**
	[-1.19]	[-1.18]
ROCE	**0.0148**	**0.2837**
	[0.15]	[1.61]
Readability	**0.1344*****	**-0.1081***
	[3.7]	[-1.78]
Secret	**0.2014***	**0.7763*****
	[1.65]	[7.15]
Risk Length Table	**0.144*****	**0.2837*****
	[4.1]	[7.02]
Volume per Cap.	**0.0006**	**0.008*****
	[0.12]	[3.59]
Humans per Cap.	**-0.0005*****	**-0.0**
	[-11.29]	[-0.64]
Year fixed effect	Yes	Yes
Industry fixed effect	No	Yes
Firm fixed effect	Yes	No
Observations	25531	25531
R^2 within	0.3099	0.2564

Table 5.5: **Determinants of firm-level credential movement cyber score**

This table reports the results of cyber score regressions on firm characteristics. Year-, industry-, and firm-fixed effects are controlled. T-statistics are reported in brackets. The variables are standardized, and the standard errors are clustered at the firm level. $*$, $**$, and $***$ indicate significance at the 10%, 5% and 1% levels, respectively. All characteristics are defined in Table A.1.

Dependent variable: Firm-level indicator of cyber score		
	Model 1	Model 2
Constant	**49.357*****	**52.308*****
	[47.79]	[65.49]
Firm Size (ln)	**-0.0327**	**0.0116**
	[-0.71]	[0.43]
Firm Age (ln)	**-0.1343**	**-0.4462*****
	[-1.2]	[-8.4]
ROA	**0.0298**	**0.1**
	[0.29]	[0.54]
Book to Market	**-0.0117**	**-0.1262*****
	[-0.96]	[-5.07]
Market Beta	**-0.0542***	**-0.127*****
	[-1.96]	[-3.29]
Intangibles/Assets	**-0.2192**	**0.9123*****
	[-1.23]	[4.78]
Debt/Assets	**-0.4056***	**1.0515*****
	[-1.85]	[2.6]
ROE	**0.0071**	**-0.0028**
	[0.16]	[-0.03]
Price/Earnings	**0.0001**	**-0.0001**
	[1.2]	[-0.29]
Profit Margin	**0.0004**	**0.0225*****
	[0.09]	[3.0]
Asset Turnover	**-0.0273**	**-0.4263*****
	[-0.36]	[-3.64]
Cash Ratio	**-0.0018**	**0.0015**
	[-0.2]	[0.11]
Sales/Invested Capital	**0.0107**	**0.1105****
	[0.34]	[2.03]
Capital Ratio	**-0.0628**	**-2.1721*****
	[-0.36]	[-7.0]
R&D/Sales	**-0.004**	**-0.0051**
	[-0.65]	[-0.54]
ROCE	**-0.0611**	**0.1708**
	[-0.72]	[1.12]
Readability	**0.1256*****	**-0.1214****
	[3.34]	[-2.15]
Secret	**0.059**	**0.6653*****
	[0.55]	[6.89]
Risk Length Table	**0.0929*****	**0.1794*****
	[3.29]	[5.55]
Volume per Cap.	**-0.0007**	**0.0056****
	[-0.21]	[2.29]
Humans per Cap.	**-0.0002*****	**-0.0**
	[-7.49]	[-0.82]
Year fixed effect	Yes	Yes
Industry fixed effect	No	Yes
Firm fixed effect	Yes	No
Observations	25531	25531
R^2 within	0.2193	0.1566

Table 5.6: **Determinants of firm-level persistence and evasion cyber score**

This table reports the results of cyber score regressions on firm characteristics. Year-, industry-, and firm-fixed effects are controlled. T-statistics are reported in brackets. The variables are standardized, and the standard errors are clustered at the firm level. $*$, $**$, and $***$ indicate significance at the 10%, 5% and 1% levels, respectively. All characteristics are defined in Table A.1.

Dependent variable: Firm-level indicator of cyber score		
	Model 1	Model 2
Constant	**48.897*****	**49.466*****
	[42.14]	[56.36]
Firm Size (ln)	**0.0069**	**0.0873*****
	[0.13]	[2.99]
Firm Age (ln)	**-0.7352*****	**-0.523*****
	[-5.92]	[-9.11]
ROA	**-0.0807**	**-0.1396**
	[-0.76]	[-0.78]
Book to Market	**-0.0347*****	**-0.1499*****
	[-2.75]	[-5.58]
Market Beta	**-0.0577***	**-0.0962****
	[-1.92]	[-2.34]
Intangibles/Assets	**-0.1576**	**1.5511*****
	[-0.73]	[7.31]
Debt/Assets	**-0.4222***	**1.6297*****
	[-1.67]	[3.81]
ROE	**0.0376**	**0.0192**
	[0.7]	[0.21]
Price/Earnings	**0.0002**	**0.0**
	[1.6]	[0.05]
Profit Margin	**-0.0009**	**0.0191*****
	[-0.21]	[2.63]
Asset Turnover	**-0.033**	**-0.4303*****
	[-0.36]	[-3.38]
Cash Ratio	**0.0055**	**0.015**
	[0.56]	[0.96]
Sales/Invested Capital	**0.0072**	**0.146****
	[0.21]	[2.46]
Capital Ratio	**0.0664**	**-2.5668*****
	[0.33]	[-7.98]
R&D/Sales	**-0.0094**	**-0.0015**
	[-1.59]	[-0.15]
ROCE	**0.0523**	**0.3945****
	[0.52]	[2.55]
Readability	**0.0651**	**-0.1943*****
	[1.64]	[-3.14]
Secret	**0.2292***	**0.6711*****
	[1.95]	[6.58]
Risk Length Table	**0.1945*****	**0.3505*****
	[5.87]	[9.16]
Volume per Cap.	**-0.0021**	**0.0036**
	[-0.53]	[1.45]
Humans per Cap.	**-0.0005*****	**0.0**
	[-10.84]	[0.44]
Year fixed effect	Yes	Yes
Industry fixed effect	No	Yes
Firm fixed effect	Yes	No
Observations	25531	25531
R^2 within	0.4331	0.3920

Table 5.7: **Determinants of firm-level preparation and reconnaissance cyber score**

This table reports the results of cyber score regressions on firm characteristics. Year-, industry-, and firm-fixed effects are controlled. T-statistics are reported in brackets. The variables are standardized, and the standard errors are clustered at the firm level. $*$, $**$, and $***$ indicate significance at the 10%, 5% and 1% levels, respectively. All characteristics are defined in Table A.1.

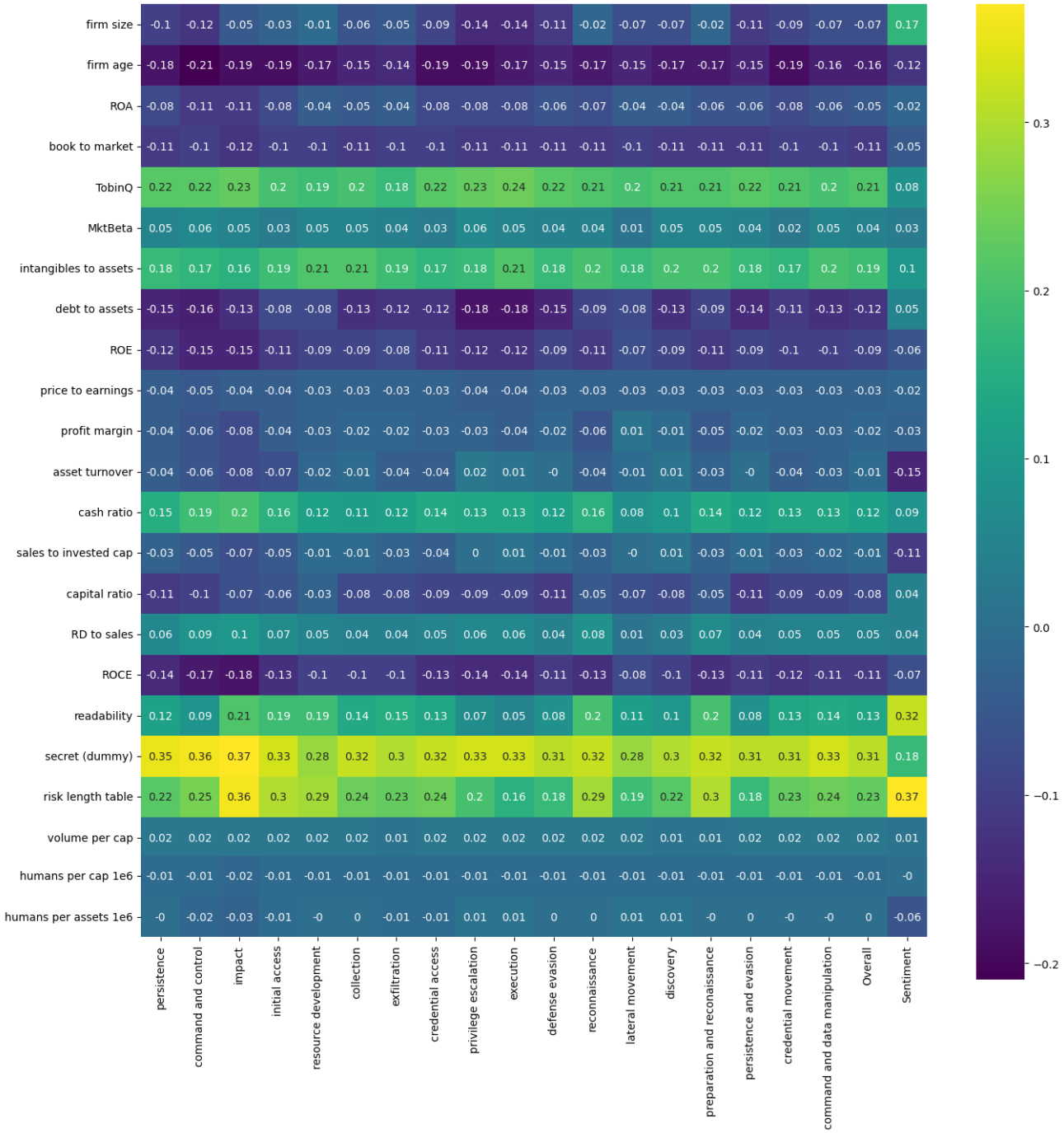

Figure 5.10: **Correlations of all cyber scores with financial characteristics**

Firm-wise correlations of the sub-cyber scores of the 14 MITRE ATT&CK tactics, the four aggregated sub-cyber scores of the super-tactics, as well as the overall cyber score and the cyber sentiment score with the financial characteristics of the firms.

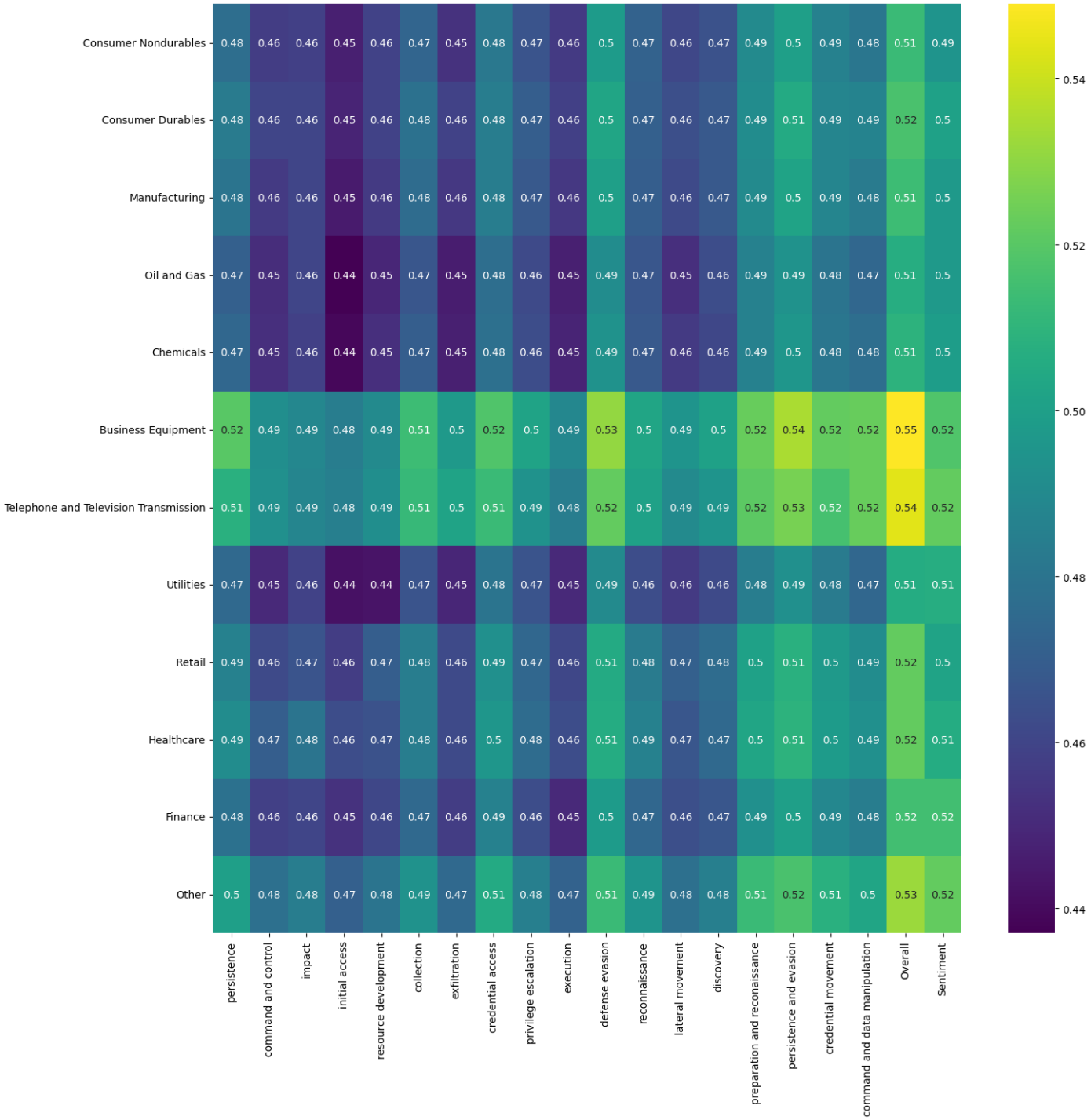

Figure 5.11: **Average cyber score across industries**

The respective average cyber scores of each firm (from 2009-Q1 to 2023-Q4) are computed and averaged across the industry the firms belong to, thus obtaining the different averaged cyber scores aggregate for each industry. Firms are classified into industries using the Fama-French 12 industry classification.

5.4 Univariate sorts

This section answers the following questions: Does a portfolio sorted according to a given cyber score display a structure in its returns? Are the pricing factors usually found in the literature enough to fully explain (not generate alphas on) the return of the cyber-based portfolios?

Tables 5.8, 5.10, 5.11, 5.12, and 5.13 all display increasing average excess returns, along with the associated cyber score, with P5 being the portfolio of firms with the highest cyber score. If a given cyber score is an adequate proxy for the associated cyber risk, it implies that taking additional cyber risk grants additional returns. This idea is further explored in the next section.

In Table 5.9, I report the average returns of portfolios sorted on the cyber sentiment score. Despite all returns being statistically significant at the 1% level, I cannot observe a monotonic increase in average returns across the scores, and P3 displays the highest average excess returns in P3. This could indicate that the score does not reflect any risk or that investors are unaware of the type of risk it reflects. I provide additional insight in the following section.

Second, Tables 5.8, 5.10, 5.11, 5.12, and 5.13, show that the linear regression using the pricing factors respectively contained in the CAPM, FFC, and FF5 models all grant a statistically significant alpha for P5 only (with statistical significance at the 5% level for CAPM and 1% level otherwise). Alphas are increasing monotonically across the portfolios after controlling for other sources of risk associated with the pricing factors involved. With this evidence in mind, the alphas could partly reflect the cyber risk of each portfolio. This is, however, not the case for the cyber sentiment score in Table 5.9 since there is no overall strong statistical significance or increasing trends when portfolios are sorted across this variable.

	P1	P2	P3	P4	P5	P5-P1
A. Portfolios sorted by cyber score						
avg. excess ret.	**0.82*****	**0.93*****	**1.04*****	**1.22*****	**1.44*****	**0.62****
	[3.27]	[3.46]	[3.65]	[4.65]	[4.54]	[2.05]
CAPM alpha	**-0.18**	**-0.12**	**-0.08**	**0.14**	**0.36****	**0.54**
	[-0.85]	[-0.93]	[-0.84]	[1.47]	[2.14]	[1.49]
FFC alpha	**-0.09**	**-0.05**	**0.0**	**0.15***	**0.27*****	**0.36****
	[-0.88]	[-0.57]	[0.04]	[1.71]	[3.04]	[2.2]
FF5 alpha	**-0.14**	**-0.1**	**0.0**	**0.13**	**0.29*****	**0.44*****
	[-1.57]	[-1.18]	[0.01]	[1.47]	[3.16]	[2.88]
B. Characteristics						
Nb. firms	628.48	629.1	629.01	629.1	629.67	-
Avg. cyber score	0.49	0.51	0.52	0.53	0.57	-
Sharp Ratio	0.61	0.69	0.72	0.88	1.02	0.68

Table 5.8: **Average monthly excess returns and alphas (in percent) using the overall cyber score**

FFC refers to the four-factor model of Carhart (1997), and FF5 refers to the five-factor model of Fama and French (2015). Panel B shows the average number of firms in each portfolio and the average cyber risk of the portfolios. T-statistics are reported in brackets. $*$, $**$, and $***$ indicate significance at the 10%, 5%, and 1% levels, respectively. The time ranges from January 2009 to December 2023.

	P1	P2	P3	P4	P5	P5-P1
A. Portfolios sorted by cyber score						
avg. excess ret.	**0.99*****	**1.08*****	**1.24*****	**1.15*****	**1.14*****	**0.14**
	[3.92]	[4.61]	[4.78]	[3.94]	[3.88]	[1.21]
CAPM alpha	**-0.03**	**0.04**	**0.19***	**0.02**	**0.05**	**0.08**
	[-0.27]	[0.31]	[1.91]	[0.31]	[0.59]	[0.58]
FFC alpha	**0.0**	**0.05**	**0.17***	**0.04**	**0.05**	**0.05**
	[0.02]	[0.48]	[1.78]	[0.59]	[0.66]	[0.45]
FF5 alpha	**-0.03**	**-0.02**	**0.12**	**0.07**	**0.1**	**0.12**
	[-0.41]	[-0.18]	[1.31]	[1.15]	[1.17]	[1.15]
B. Characteristics						
Nb. firms	628.48	629.1	629.01	629.1	629.67	-
Avg. cyber score	0.46	0.49	0.51	0.53	0.57	-
Sharp Ratio	0.75	0.8	0.92	0.81	0.82	0.3

Table 5.9: **Average monthly excess returns and alphas (in percent) using the cyber sentiment score**

	P1	P2	P3	P4	P5	P5-P1
A. Portfolios sorted by cyber score						
avg. excess ret.	**0.81*****	**0.91*****	**1.12*****	**1.17*****	**1.46*****	**0.65***
	[3.18]	[3.35]	[4.31]	[4.55]	[4.33]	[1.94]
CAPM alpha	**-0.22**	**-0.13**	**0.06**	**0.05**	**0.39****	**0.6**
	[-0.94]	[-1.07]	[0.75]	[0.61]	[2.01]	[1.49]
FFC alpha	**-0.11**	**-0.07**	**0.1****	**0.04**	**0.3*****	**0.42****
	[-1.0]	[-0.77]	[2.18]	[0.5]	[2.69]	[2.12]
FF5 alpha	**-0.16**	**-0.12**	**0.11****	**0.03**	**0.33*****	**0.49*****
	[-1.66]	[-1.35]	[2.01]	[0.37]	[2.76]	[2.61]
B. Characteristics						
Nb. firms	628.48	629.1	629.01	629.1	629.67	-
Avg. cyber score	0.46	0.48	0.49	0.5	0.54	-
Sharp Ratio	0.59	0.68	0.82	0.82	1.04	0.71

Table 5.10: **Average monthly excess returns and alphas (in percent) using the command and data manipulation cyber score**

	P1	P2	P3	P4	P5	P5-P1
A. Portfolios sorted by cyber score						
avg. excess ret.	**0.88*****	**0.9*****	**1.04*****	**1.13*****	**1.49*****	**0.61****
	[3.63]	[3.51]	[3.5]	[4.34]	[4.66]	[2.06]
CAPM alpha	**-0.12**	**-0.14**	**-0.1**	**0.07**	**0.4****	**0.52**
	[-0.6]	[-1.01]	[-1.16]	[1.11]	[2.31]	[1.48]
FFC alpha	**-0.04**	**-0.07**	**-0.02**	**0.09**	**0.3*****	**0.34****
	[-0.41]	[-0.76]	[-0.29]	[1.4]	[3.09]	[2.07]
FF5 alpha	**-0.1**	**-0.11**	**-0.02**	**0.08**	**0.33*****	**0.43*****
	[-1.15]	[-1.25]	[-0.32]	[1.23]	[3.19]	[2.74]
B. Characteristics						
Nb. firms	628.48	629.1	629.01	629.1	629.67	-
Avg. cyber score	0.46	0.48	0.49	0.51	0.54	-
Sharp Ratio	0.66	0.67	0.72	0.83	1.04	0.69

Table 5.11: **Average monthly excess returns and alphas (in percent) using the credential movement cyber score**

	P1	P2	P3	P4	P5	P5-P1
A. Portfolios sorted by cyber score						
avg. excess ret.	**0.84*****	**0.95*****	**1.04*****	**1.11*****	**1.49*****	**0.64****
	[3.35]	[3.61]	[3.75]	[4.44]	[4.54]	[2.01]
CAPM alpha	**-0.18**	**-0.08**	**-0.03**	**0.05**	**0.39****	**0.58**
	[-0.86]	[-0.54]	[-0.39]	[0.66]	[2.16]	[1.53]
FFC alpha	**-0.1**	**0.01**	**0.03**	**0.08**	**0.29*****	**0.39****
	[-0.89]	[0.13]	[0.38]	[1.47]	[2.9]	[2.23]
FF5 alpha	**-0.15**	**-0.05**	**0.03**	**0.05**	**0.33*****	**0.48*****
	[-1.66]	[-0.78]	[0.5]	[0.78]	[3.09]	[2.97]
B. Characteristics						
Nb. firms	628.48	629.1	629.01	629.1	629.67	-
Avg. cyber score	0.48	0.49	0.5	0.52	0.55	-
Sharp Ratio	0.61	0.71	0.76	0.82	1.03	0.67

Table 5.12: **Average monthly excess returns and alphas (in percent) using the persistence and evasion cyber score**

	P1	P2	P3	P4	P5	P5-P1
A. Portfolios sorted by cyber score						
avg. excess ret.	**0.86*****	**0.85*****	**1.15*****	**1.11*****	**1.43*****	**0.57****
	[3.54]	[3.13]	[4.22]	[3.94]	[4.69]	[1.97]
CAPM alpha	**-0.09**	**-0.23**	**0.02**	**0.02**	**0.37****	**0.46**
	[-0.44]	[-1.97]	[0.2]	[0.29]	[2.39]	[1.34]
FFC alpha	**-0.02**	**-0.16**	**0.07**	**0.04**	**0.28*****	**0.3***
	[-0.14]	[-2.45]	[1.23]	[0.56]	[3.07]	[1.75]
FF5 alpha	**-0.09**	**-0.19**	**0.11***	**0.01**	**0.3*****	**0.38****
	[-0.95]	[-3.08]	[1.76]	[0.19]	[3.17]	[2.42]
B. Characteristics						
Nb. firms	628.48	629.1	629.01	629.1	629.67	-
Avg. cyber score	0.47	0.48	0.5	0.51	0.54	-
Sharp Ratio	0.67	0.61	0.8	0.8	1.03	0.69

Table 5.13: **Average monthly excess returns and alphas (in percent) using the preparation and reconnaissance cyber score**

5.5 Double sorts

I aim to determine if organizing quarterly portfolios first based on specific characteristics and then based on the cyber score results in a structure in their average excess returns. The idea is that controlling for additional characteristics rejects the hypothesis that the cyber scores are a proxy for another firm variable. Thus, the cyber score would capture the cyber risk exposure and the associated additional returns. In other words, the increasing cyber score, which should reflect the increasing cyber risk, still displays increasing related returns even if the set of firms to analyze is already organized and structured according to another characteristic unrelated to cyber risk.

Table 5.14 displays the average returns of various double-sorted portfolios. Notably, there is a clear increasing trend in average returns as the overall cyber score quintile increases, which contrasts with the findings of Celeny and Maréchal (2023), where the trend was less pronounced. In my analysis, only the first quintile of the book-to-market ratio does not consistently show an increase. Note that Q3 of market beta and Q5 of the size have a difference problem of 0.01% at Q3. However, this quantitatively marginal result may be spurious.

For the cyber sentiment score, as previously observed in Table 5.9, there are no additional returns for an increase in the score, so the cyber sentiment score certainly does not reflect any risk.

The returns obtained with other cyber scores display an interesting aspect. Command and data manipulation, credential movement, and persistence and evasion strongly suggest a monotonic increasing trend and, therefore, cyber risks premia, except for the lower quintile, where the conclusion might seem slightly less evident. However, this is not the case for preparation and reconnaissance, for which the trend is nonmonotonic almost everywhere. This could suggest two things. It could be that investors do not acknowledge the risk this cyber score reflects. Or, it could be that preparation and reconnaissance do not reflect any risk.

	Q1	**Q2**	**Q3**	**Q4**	**Q5**		**Q1**	**Q2**	**Q3**	**Q4**	**Q5**		**Q1**	**Q2**	**Q3**	**Q4**	**Q5**
Double sorted portfolios with overall cyber score																	
Beta Q1	1.01	1.01	1.13	1.37	1.42	BM Q1*	1.09	0.98	1.14	1.18	1.24	Size Q1	0.86	0.96	1.06	1.22	1.32
Beta Q2	0.89	1.00	1.07	1.25	1.33	BM Q2	0.86	0.92	1.01	1.25	1.37	Size Q2	0.87	0.96	1.05	1.25	1.32
Beta Q3	0.89	1.02	1.01	1.22	1.28	BM Q3	0.85	1.01	1.04	1.23	1.33	Size Q3	0.87	0.95	1.05	1.25	1.32
Beta Q4	0.84	0.90	1.04	1.23	1.25	BM Q4	0.83	0.99	1.03	1.22	1.35	Size Q4	0.86	0.95	1.08	1.26	1.33
Beta Q5	0.83	0.92	1.02	1.21	1.30	BM Q5	0.87	0.95	1.07	1.22	1.33	Size Q5	1.09	1.15	1.20	1.19	1.39
Double sorted portfolios with cyber sentiment score																	
Beta Q1	1.16	1.23	1.27	1.25	1.09	BM Q1*	1.13	1.15	1.04	1.12	1.12	Size Q1*	0.97	1.20	1.10	1.15	1.07
Beta Q2*	0.95	1.00	1.36	1.18	1.07	BM Q2*	0.93	1.01	1.30	1.13	1.09	Size Q2*	0.96	1.12	1.21	1.13	1.07
Beta Q3*	1.06	1.00	1.07	1.11	1.10	BM Q3*	0.96	1.13	1.22	1.15	1.08	Size Q3*	0.96	1.11	1.19	1.13	1.07
Beta Q4*	0.95	1.08	1.10	1.09	1.03	BM Q4*	0.95	1.09	1.21	1.14	1.08	Size Q4*	0.95	1.03	1.24	1.11	1.08
Beta Q5*	0.96	1.00	1.20	1.13	1.04	BM Q5*	0.95	1.09	1.20	1.15	1.05	Size Q5*	1.23	1.16	1.20	1.17	1.29
Double sorted portfolios with command and data manipulation cyber score																	
Beta Q1	1.04	1.06	1.18	1.27	1.41	BM Q1*	1.07	0.94	1.22	1.15	1.24	Size Q1	0.90	0.89	1.16	1.13	1.33
Beta Q2	0.89	0.93	1.14	1.19	1.36	BM Q2	0.83	0.89	1.11	1.16	1.39	Size Q2*	0.89	0.91	1.16	1.12	1.33
Beta Q3*	0.91	0.90	1.16	1.09	1.34	BM Q3	0.89	0.90	1.17	1.16	1.34	Size Q3	0.87	0.91	1.16	1.14	1.34
Beta Q4	0.85	0.85	1.17	1.14	1.25	BM Q4	0.85	0.93	1.15	1.20	1.32	Size Q4	0.85	0.96	1.11	1.21	1.34
Beta Q5	0.87	0.85	1.11	1.12	1.30	BM Q5	0.86	0.96	1.13	1.20	1.31	Size Q5	1.11	1.19	1.16	1.16	1.41
Double sorted portfolios with credential movement cyber score																	
Beta Q1*	1.05	0.96	1.16	1.22	1.49	BM Q1*	1.03	1.03	1.18	1.09	1.25	Size Q1	0.90	0.93	1.06	1.10	1.39
Beta Q2*	0.93	0.94	1.08	1.03	1.42	BM Q2	0.86	0.90	1.07	1.16	1.41	Size Q2	0.90	0.92	1.09	1.09	1.38
Beta Q3	0.90	0.99	1.03	1.08	1.37	BM Q3	0.93	0.92	1.05	1.09	1.41	Size Q3	0.90	0.92	1.08	1.08	1.40
Beta Q4	0.85	0.88	1.09	1.09	1.31	BM Q4	0.90	0.90	1.07	1.09	1.41	Size Q4	0.89	0.93	1.03	1.10	1.42
Beta Q5	0.90	0.87	1.04	1.11	1.35	BM Q5	0.88	0.95	1.06	1.06	1.41	Size Q5	1.13	1.13	1.17	1.22	1.39
Double sorted portfolios with persistence and evasion cyber score																	
Beta Q1*	1.02	1.07	1.12	1.25	1.46	BM Q1*	1.06	1.01	1.18	1.19	1.19	Size Q1	0.88	0.99	1.08	1.12	1.36
Beta Q2*	0.88	1.06	1.05	1.13	1.40	BM Q2*	0.85	1.03	0.98	1.19	1.41	Size Q2	0.89	1.00	1.08	1.15	1.34
Beta Q3	0.90	1.05	1.06	1.09	1.33	BM Q3	0.90	1.00	1.03	1.15	1.38	Size Q3	0.88	0.99	1.05	1.14	1.38
Beta Q4	0.86	0.97	1.05	1.11	1.29	BM Q4	0.87	1.00	1.03	1.17	1.38	Size Q4	0.86	1.02	1.05	1.14	1.39
Beta Q5	0.87	0.91	0.99	1.18	1.32	BM Q5	0.86	1.00	1.05	1.16	1.38	Size Q5	1.17	1.10	1.20	1.16	1.39
Double sorted portfolios with preparation and reconnaissance cyber score																	
Beta Q1*	1.10	0.91	1.28	1.21	1.41	BM Q1*	1.08	0.99	1.12	1.13	1.24	Size Q1*	0.91	0.84	1.13	1.15	1.34
Beta Q2*	0.93	0.87	1.20	1.13	1.35	BM Q2*	0.85	0.78	1.18	1.19	1.37	Size Q2*	0.92	0.83	1.14	1.20	1.31
Beta Q3	0.92	0.90	1.13	1.11	1.29	BM Q3*	0.90	0.93	1.15	1.09	1.34	Size Q3*	0.90	0.87	1.17	1.13	1.32
Beta Q4*	0.90	0.77	1.20	1.07	1.27	BM Q4	0.86	0.89	1.15	1.12	1.34	Size Q4*	0.86	0.86	1.20	1.12	1.34
Beta Q5*	0.89	0.78	1.13	1.12	1.29	BM Q5	0.85	0.90	1.13	1.14	1.34	Size Q5	1.13	1.15	1.19	1.19	1.38

Table 5.14: **Average returns of the double sorted portfolios**

Q1 to **Q5** represent quintiles. The sorting of firms is done according to market beta (Beta), book-to-market ratios (BM), or firm size (Size) and then on the relevant cyber score. The average returns are given in percent. $*$ indicates that the returns are not increasing monotonically with the quintile of the cyber score (with an incertitude of -0.03%).

5.6 Cross-sectional tests

I test whether a cyber score increase drives a return increase in cyber-based portfolios, controlling for other well-known pricing factors using the regression method described in Fama and MacBeth (1973). Table 5.15, 5.16, 5.17, 5.18, 5.19, and 5.20 displays the results for each cyber score using a different pricing model that include the cyber score.

The cyber sentiment score probably reflects no meaningful reality regarding the firms; therefore, constructing portfolios based on it reveals no particular structure, as observed in Table 5.16. No risk premia is observed for any of the involved pricing factors (including the cyber sentiment score), and no statistically significant alpha exists.

The overall cyber score on Table 5.15 displays positive additional returns for an increased cyber score that is statistically significant at the 10% level when included as the only explanatory variable or with the market factor and at the 5% level when included with the pricing factors from Fama and French (1992). However, a collinearity problem appears for the fifth model using additional factors from Fama and French (2015). The cyber score aggregated for all the firms of the cyber-based portfolios constructs a factor that might be colinear to CMA. Therefore, the statistical significance of the cyber score is affected and strongly reduced. When compared to Celeny and Maréchal (2023), they appear to not suffer from collinearity and have a less high adjusted R^2.

The command and data manipulation score on Table 5.17 grants similar results, also suffering from collinearity. On the contrary, the remaining score in Tables 5.18, 5.19 and 5.20 do not display collinearity and their respective cyber score appear statistically significant at the 5% level. Note that on all Tables (except for the cyber sentiment score), the coefficients of the cyber score appear positive, further pointing toward cyber scores that effectively reflect cyber risks rewarded on the market. A standard deviation of the overall cyber score (0.03 in Table 5.1) generates an additional return of $0.03 \cdot 0.04 = 0.12\%$ compared to Celeny and Maréchal (2023) with 0.18%.

	M.1	M.2	M.3	M.4	M.5
Market	**0.011*****		**0.009****	**0.013*****	**0.009****
	[2.886]		[2.526]	[3.507]	[2.429]
Cyber		**0.054***	**0.051***	**0.051****	**0.04**
		[1.925]	[1.807]	[2.097]	[1.547]
HML				**0.003**	**0.003**
				[1.176]	[0.964]
SMB				**-0.001**	**0.001**
				[-0.223]	[0.636]
UMD				**0.002**	
				[0.766]	
CMA					**-0.001**
					[-0.627]
RMW					**0.002**
					[0.776]
Constant	**0.001**	**-0.017**	**-0.024**	**-0.029****	**-0.019**
	[0.148]	[-1.083]	[-1.586]	[-2.223]	[-1.357]
$\overline{R^2_{\text{adj}}}$	0.067	0.158	0.22	0.296	0.309
MAPE	0.013	0.012	0.012	0.01	0.009

Table 5.15: **Fama-MacBeth for overall cyber score**

This table reports the results of Fama-MacBeth regressions of 20 value-weighted portfolios sorted on their cyber score. These portfolios are regressed each month on portfolio value-weighted betas with the market, HML, SMB, MOM, RMW, and CMA. "Cyber" is the value-weighted cyber score of each portfolio. HML and SMB refer to the book-to-market and size factors from Fama and French (1992). UMD refers to the momentum factor from Carhart (1997). CMA and RMW refer to the investment and operating profitability factors from Fama and French (2015). $\overline{R^2_{\text{adj}}}$ is the average adjusted R-squared, and MAPE is the mean average pricing error (mean average of the absolute value of the residuals). T-statistics are reported in brackets. *, **, and *** indicate significance at the 10%, 5% and 1% levels, respectively. The period is from January 2009 to December 2023.

	M.1	M.2	M.3	M.4	M.5
Market	**0.005**		**0.004**	**0.005**	**0.005**
	[1.335]		[0.951]	[1.308]	[1.27]
Cyber		**0.003**	**0.0**	**0.003**	**-0.008**
		[0.277]	[0.003]	[0.228]	[-0.501]
HML				**0.001**	**-0.001**
				[0.381]	[-0.235]
SMB				**0.001**	**0.001**
				[0.304]	[0.383]
UMD				**0.005**	
				[1.508]	
CMA					**-0.001**
					[-0.488]
RMW					**0.001**
					[0.486]
Constant	**0.006**	**0.01**	**0.008**	**0.005**	**0.011**
	[1.643]	[1.607]	[1.209]	[0.754]	[1.439]
$\overline{R^2_{\text{adj}}}$	0.077	0.042	0.108	0.202	0.237
MAPE	0.013	0.013	0.012	0.011	0.01

Table 5.16: **Fama-McBeth for cyber sentiment score**

	M.1	M.2	M.3	M.4	M.5
Market	**0.009****		**0.007***	**0.009****	**0.01****
	[2.328]		[1.716]	[2.493]	[2.574]
Cyber		**0.044***	**0.051***	**0.056****	**0.038**
		[1.673]	[1.914]	[2.335]	[1.401]
HML				**0.003**	**0.003**
				[1.122]	[0.942]
SMB				**0.002**	**0.002**
				[0.884]	[0.692]
UMD				**0.0**	
				[0.005]	
CMA					**-0.001**
					[-0.35]
RMW					**0.001**
					[0.561]
Constant	**0.003**	**-0.01**	**-0.02**	**-0.026****	**-0.016**
	[0.661]	[-0.733]	[-1.439]	[-2.032]	[-1.141]
$\overline{R^2_{\text{adj}}}$	0.053	0.154	0.206	0.315	0.322
MAPE	0.014	0.013	0.012	0.01	0.01

Table 5.17: **Fama-McBeth for command and data manipulation cyber score**

	M.1	M.2	M.3	M.4	M.5
Market	**0.007****		**0.004**	**0.009****	**0.007***
	[2.106]		[1.036]	[2.454]	[1.894]
Cyber		**0.051***	**0.056****	**0.065****	**0.056****
		[1.906]	[2.101]	[2.419]	[2.062]
HML				**0.005***	**0.003**
				[1.67]	[1.162]
SMB				**-0.001**	**0.001**
				[-0.379]	[0.46]
UMD				**-0.001**	
				[-0.243]	
CMA					**-0.002**
					[-1.145]
RMW					**0.001**
					[0.458]
Constant	**0.004**	**-0.014**	**-0.02**	**-0.03****	**-0.023**
	[1.04]	[-0.982]	[-1.487]	[-2.228]	[-1.649]
$\overline{R^2_{\text{adj}}}$	0.057	0.157	0.219	0.308	0.313
MAPE	0.013	0.013	0.012	0.01	0.009

Table 5.18: **Fama-McBeth for credential movement cyber score**

	M.1	M.2	M.3	M.4	M.5
Market	**0.004**		**0.002**	**0.004**	**0.003**
	[1.201]		[0.472]	[1.222]	[0.801]
Cyber		**0.056***	**0.061****	**0.073****	**0.071****
		[1.835]	[2.062]	[2.451]	[2.193]
HML				**0.003**	**0.004**
				[1.255]	[1.357]
SMB				**0.001**	**0.001**
				[0.442]	[0.474]
UMD				**-0.002**	
				[-0.477]	
CMA					**-0.0**
					[-0.192]
RMW					**0.002**
					[1.370]
Constant	**0.007**	**-0.017**	**-0.021**	**-0.03***	**-0.028**
	[1.644]	[-1.04]	[-1.349]	[-1.944]	[-1.641]
$\overline{R^2_{\text{adj}}}$	0.058	0.167	0.215	0.3	0.304
MAPE	0.013	0.012	0.012	0.01	0.009

Table 5.19: **Fama-McBeth for persistence and evasion cyber score**

	M.1	M.2	M.3	M.4	M.5
Market	**0.009***		**0.006**	**0.011****	**0.01****
	[1.951]		[1.531]	[2.541]	[2.055]
Cyber		**0.047***	**0.046***	**0.049****	**0.052****
		[1.848]	[1.888]	[2.262]	[2.299]
HML				**0.003**	**0.004**
				[1.053]	[1.52]
SMB				**0.001**	**0.001**
				[0.233]	[0.418]
UMD				**0.001**	
				[0.168]	
CMA					**-0.001**
					[-0.466]
RMW					**0.002**
					[0.862]
Constant	**0.003**	**-0.012**	**-0.018**	**-0.024****	**-0.025****
	[0.674]	[-0.908]	[-1.345]	[-2.047]	[-2.008]
$\overline{R^2_{\text{adj}}}$	0.072	0.137	0.201	0.274	0.288
MAPE	0.014	0.013	0.012	0.01	0.01

Table 5.20: **Fama-McBeth for preparation and reconaissance cyber score**

5.7 Time series tests

I want to examine whether adding the long-short portfolio $P5 - P1$ as a pricing factor enhances the explanatory power of the five-factor model of Fama and French (2015). Using the GRS test, I want to test if I can globally reduce the unexplained part of returns (the alphas) close to zero. I conduct four GRS tests on 20 portfolios sorted quarterly, on firms' cyber score, size, market beta, and book-to-market, respectively.

Tables 5.21, 5.22, 5.23, 5.24, 5.25 and 5.26 display the four GRS tests for each cyber score of interest. All tables give similar results, with the probability of alphas being commonly zero increasing as I add the cyber factor P5-P1 and the average R^2 increasing. There is an exception when portfolios are sorted on size. Their associated probabilities seem to decrease, but it is important to note that the probability is already high before adding the cyber factor. It is hard to quantify if the alphas are closer to zero when they are already commonly near zero. Also, note that the difference of probabilities in the case of market beta is positive but small compared to the improvement provided by the cyber factor when explaining the return of portfolios sorted on the cyber score or the book to market.

	GRS	p-value	$\overline{R2}$	GRS	p-value	$\overline{R2}$
	Sorted on cyber score			Sorted on size		
FF5	1.451	0.107	0.868	0.737	0.783	0.876
FF5 + CyberFactor	1.088	0.367	0.888	0.833	0.671	0.877
	Sorted on market beta			Sorted on book-to-market		
FF5	1.541	0.075	0.793	1.240	0.229	0.891
FF5 + CyberFactor	1.495	0.090	0.806	1.021	0.441	0.895

Table 5.21: **GRS test for overall cyber score**

This table reports the results of time series regressions of 20 value-weighted portfolios (sorted on the cyber score, the size of firms, the market beta or the book-to-market ratio) on the five-factor model ofFama and French (2015) (FF5) and the "CyberFactor", *i.e.* the factor built as the long-short of extreme quintile portfolios sorted on the relevant cyber score (P5-P1). The p-value is the probability that the alphas of the 20 regressions are jointly zero. A probability lower than 10% means that the hypothesis that alphas are jointly zero can be rejected at the 10% level. The study period is from January 2009 to December 2023.

	GRS	p-value	$\overline{R2}$	GRS	p-value	$\overline{R2}$
	Sorted on cyber score			Sorted on size		
FF5	1.254	0.218	0.854	0.737	0.783	0.876
FF5 + CyberFactor	1.198	0.263	0.864	0.748	0.771	0.877
	Sorted on market beta			Sorted on book-to-market		
FF5	1.541	0.075	0.793	1.240	0.229	0.891
FF5 + CyberFactor	1.488	0.093	0.796	1.188	0.271	0.892

Table 5.22: **GRS test for cyber sentiment score**

	GRS	p-value	$\overline{R2}$	GRS	p-value	$\overline{R2}$
	Sorted on cyber score			Sorted on size		
FF5	1.558	0.070	0.855	0.737	0.783	0.876
FF5 + CyberFactor	1.119	0.335	0.877	0.844	0.657	0.877
	Sorted on market beta			Sorted on book-to-market		
FF5	1.541	0.075	0.793	1.240	0.229	0.891
FF5 + CyberFactor	1.472	0.099	0.807	1.026	0.436	0.895

Table 5.23: **GRS test for command and data manipulation cyber score**

	GRS	p-value	$\overline{R2}$	GRS	p-value	$\overline{R2}$
	Sorted on cyber score			Sorted on size		
FF5	1.539	0.076	0.864	0.737	0.783	0.876
FF5 + CyberFactor	1.192	0.268	0.884	0.770	0.746	0.877
	Sorted on market beta			Sorted on book-to-market		
FF5	1.541	0.075	0.793	1.240	0.229	0.891
FF5 + CyberFactor	1.441	0.111	0.804	0.997	0.469	0.895

Table 5.24: **GRS test for credential movement**

	GRS	p-value	$\overline{R2}$	GRS	p-value	$\overline{R2}$
	Sorted on cyber score			Sorted on size		
FF5	1.465	0.101	0.868	0.737	0.783	0.876
FF5 + CyberFactor	1.128	0.326	0.890	0.884	0.608	0.878
	Sorted on market beta			Sorted on book-to-market		
FF5	1.541	0.075	0.793	1.240	0.229	0.891
FF5 + CyberFactor	1.500	0.088	0.806	1.021	0.441	0.896

Table 5.25: **GRS test for persistence and evasion cyber score**

	GRS	p-value	$\overline{R2}$	GRS	p-value	$\overline{R2}$
	Sorted on cyber score			Sorted on size		
FF5	1.516	0.083	0.861	0.737	0.783	0.876
FF5 + CyberFactor	1.216	0.248	0.879	0.807	0.703	0.877
	Sorted on market beta			Sorted on book-to-market		
FF5	1.541	0.075	0.793	1.240	0.229	0.891
FF5 + CyberFactor	1.546	0.076	0.807	0.990	0.477	0.896

Table 5.26: **GRS test for preparation and reconaissance cyber score**

5.8 Bayesian asset pricing tests

I conduct an additional test to evaluate the cyber factor P5-P1 as a reliable pricing factor. Using the Bayesian GRS (BGRS) test described earlier, I can retrieve the best subset of pricing factors among a large set of pricing factors. Figures 5.12, 5.13, 5.14, 5.15, 5.16 and 5.17 presents the BGRS test for each cyber score of interest. Keeping only the subsets with the higher probabilities at the end of the time range, one can notice that the top five subsets always include the cyber factor (except for the cyber sentiment score case, where one of the top five subsets does not include the cyber factor). When considering the cumulative probabilities associated with each pricing factor, one can see that the cyber factors have always presented a growing trend over the years, meaning that the cyber factors have become more relevant as a pricing factor over time.

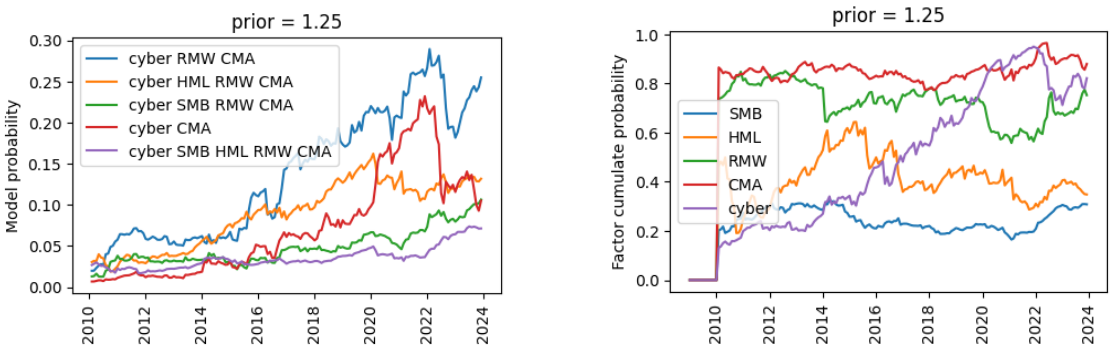

Figure 5.12: **Factor model posterior probabilities using overall cyber score**

The first figure depicts the probabilities of being a better set of pricing factors for the shown subset compared to all possible subsets of factors. I present only the top five models, ranked by the probability at the end of the sample, meaning that all other subsets have lower pricing abilities than the ones presented here. HML and SMB refer to the book-to-market and size factors of Fama and French (1992). CMA and RMW refer to the investment and operating profitability factors of Fama and French (2015). "cyber" refers to the long-short portfolio built on the cyber score of interest (P5-P1). The prior multiple is 1.25, and the study period is from January 2010 to December 2022. The second figure shows the cumulative probabilities, *i.e.* the sum of probabilities of all the pricing subsets containing the factor on a similar time range.

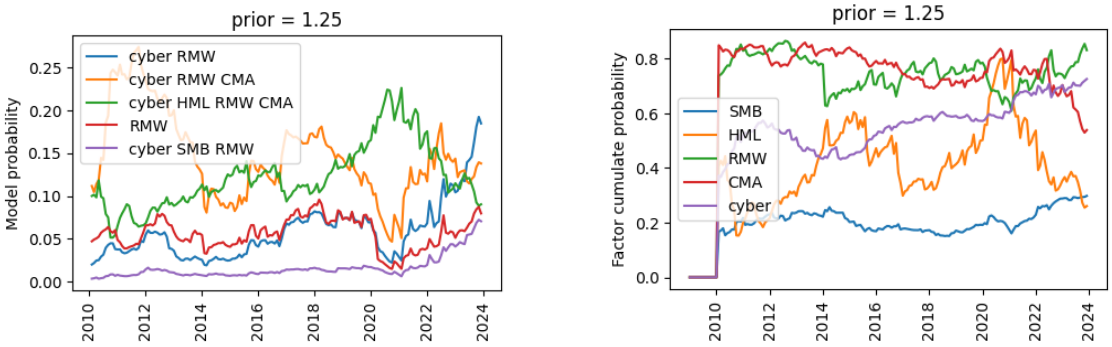

Figure 5.13: **Factor model posterior probabilities using cyber sentiment score**

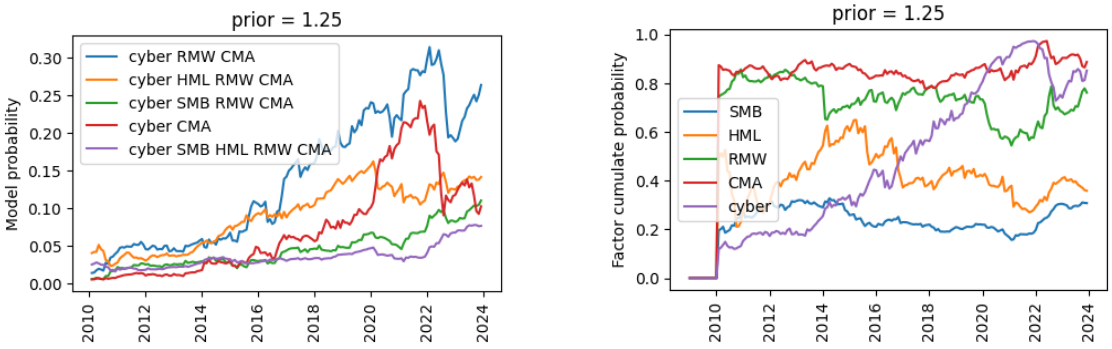

Figure 5.14: **Factor model posterior probabilities using command and data manipulation cyber score**

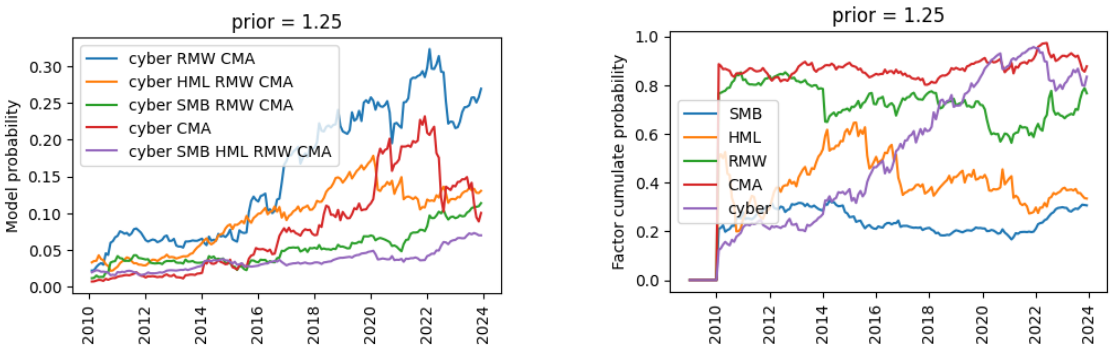

Figure 5.15: **Factor model posterior probabilities using credential movement cyber score**

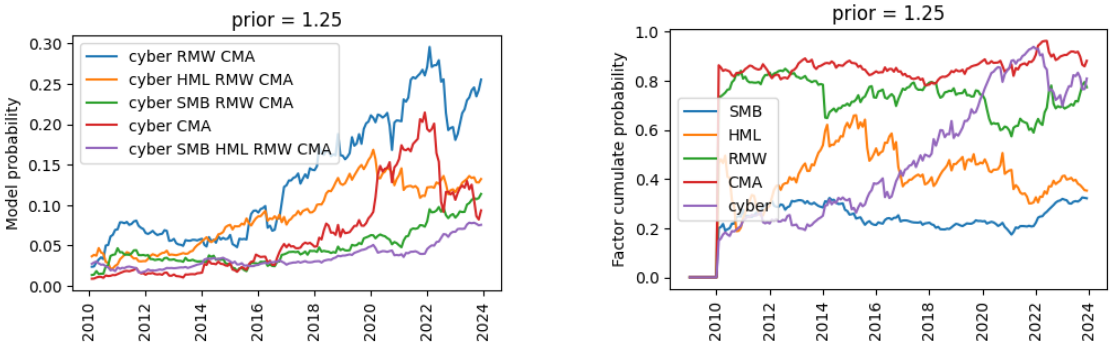

Figure 5.16: **Factor model posterior probabilities using persistence and evasion cyber score**

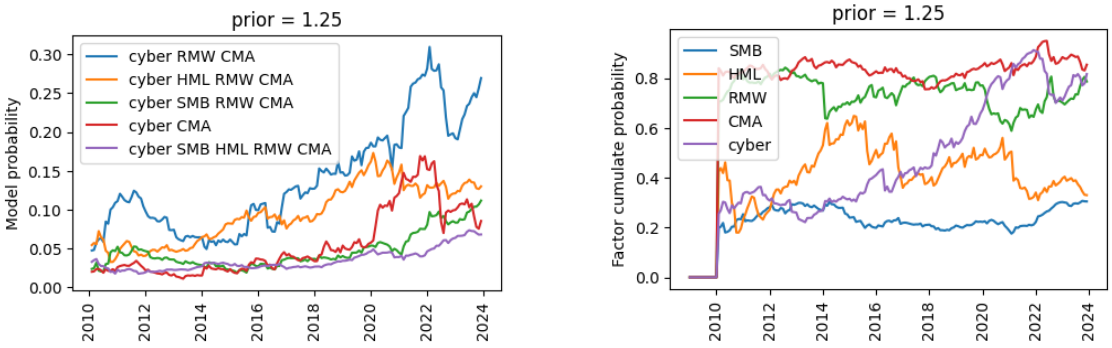

Figure 5.17: **Factor model posterior probabilities using preparation and reconnaissance cyber score**

5.9 Additional tests

In this section, I conduct further tests to expand the range and depth of understanding of the cyber scores I developed. These additional tests aim to identify any potential limitations and verify the scores' behavior in a real case.

Cyber score	P5 (top 20%)		P20 (top 5%)	
	t-stat.	p-value	t-stat.	p-value
persistence	-0.0372	0.9703	-0.0768	0.9388
command and control	0.0605	0.9518	0.7315	0.4649
impact	0.0692	0.9449	0.0011	0.9992
initial access	-0.0751	0.9402	0.1292	0.8972
resource development	0.3001	0.7643	0.2834	0.7770
collection	-0.0099	0.9921	0.0890	0.9291
exfiltration	0.0041	0.9967	0.4411	0.6593
credential access	-0.0167	0.9867	0.3022	0.7626
privilege escalation	-0.0461	0.9632	0.1641	0.8697
execution	0.2384	0.8117	0.1040	0.9172
defense evasion	0.0474	0.9622	-0.1037	0.9174
reconnaissance	0.1565	0.8757	0.2418	0.8091
lateral movement	-0.0665	0.9470	-0.2061	0.8368
discovery	0.0419	0.9666	0.1053	0.9162
preparation and reconnaissance	0.1050	0.9165	0.2395	0.8108
persistence and evasion	-0.1185	0.9058	-0.0888	0.9293
credential movement	0.0242	0.9807	-0.0176	0.9860
command and data manipulation	0.0894	0.9288	0.0601	0.9521
sentiment	0.6125	0.5405	1.1653	0.2446

Table 5.27: **Cyber based portfolio returns differences**

The table displays the outcomes of Welch's t-test, the statistical method used to evaluate the significance of mean differences with the possibility of different variances, applied to each cyber score time series in comparison to the overall cyber score time series. These time series are the monthly returns of cyber-based portfolios: P5 (constructed with 5 quantiles, taking the top 20%) and P20 (constructed with 20 quantiles, taking the top 5%).

In Table 5.27, I display the probabilities associated with the differences in mean returns between the overall and other cyber-based portfolios. Although I demonstrated that the cyber scores indeed reflect different realities related to the cyber subject in the 10-Ks, it seems that when portfolios are constructed from these scores, their returns do not display any statistically significant variation across different scores. In the context of market perception of risk, the results of the table suggest there is no distinction between the various domains of cyber risk, and the market perceives a single aggregated risk related to cybersecurity.

In December 2020, a significant cyber attack on SolarWinds, a major IT management company, was uncovered, marking one of the most extensive and sophisticated cyber espionage operations to date. The attackers believed to be state-sponsored, infiltrated SolarWinds' Orion software, which was used by numerous high-profile clients, including Fortune 500 companies and various U.S. government agencies. By embedding malicious code in a routine software update, the attackers gained unprecedented access to sensitive data across multiple networks. This breach not only highlighted vulnerabilities within supply chain security but also underscored the broader implications for firms at risk of cyber attacks. The incident serves as a case study for analyzing the financial impact on companies deemed to be cyber-risky. Such analysis using this event was performed in Florackis et al. (2023) where they analyzed cumulative abnormal returns from their cyber-based portfolios setting the 14 December 2020, the day where the attack was disclosed to the SEC, as the t=0 day of the event.

	P1	P2	P3	P4	P5	P5-P1
CAR[-1,1]	-0.146	0.001	-0.021	-0.103	0.206	0.352
t-statistic	-0.311	0.002	-0.058	-0.342	0.616	0.450
CAR[-1,3]	-0.197	-0.040	-0.178	-0.051	0.194	0.390
t-statistic	-0.540	-0.115	-0.626	-0.220	0.748	0.644

Table 5.28: **Cumulative abnormal returns of cyber-based portfolios**

To estimate the cumulative abnormal returns (CAR), I use the market model around December 14, 2020, as t=0. Note that it was a Monday. Therefore, $t = -1$ corresponds to Friday, December 11. The beta of the market model is set up thanks to the returns of the prior year. The abnormal returns are given in percent. The portfolios are based on the overall cyber score.

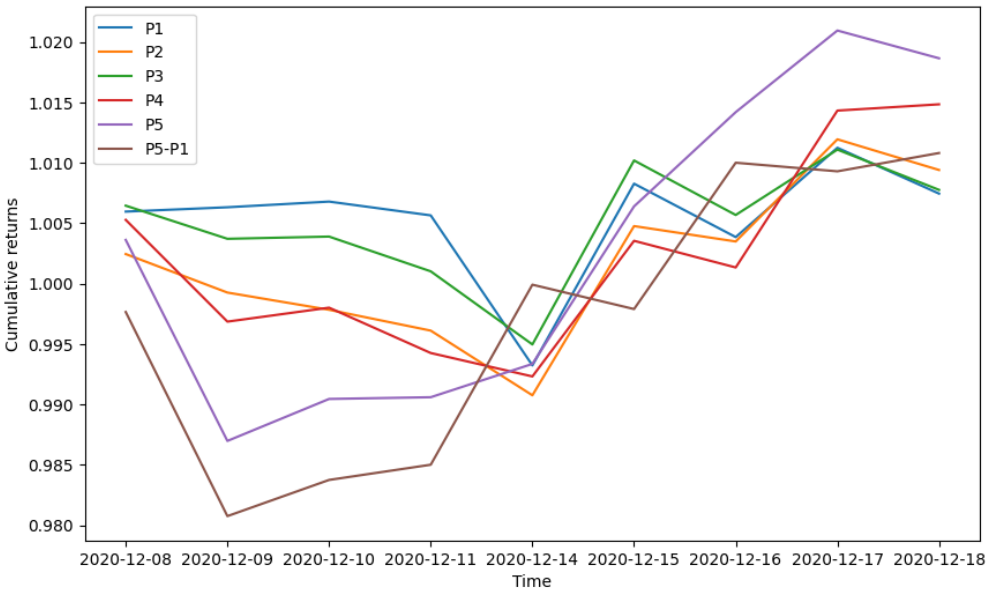

Figure 5.18: **Cumulative returns of cyber-based portfolio around SolarWinds breach**

Evolution of the portfolio based on the overall cyber score if 1 dollar was invested the December 7, 2020. Note that the closed trading days do not appear.

I conduct a similar analysis on Table 5.28. None of the abnormal returns were statistically significant. Figure 5.18 illustrates the cumulative returns of the cyber-based portfolio around this event. The results are unconventional. Returns were higher in the lower-tier cyber-based portfolio in the days leading up to the event. Moreover, when the event occurred, all portfolios declined except for P5. However, two important factors need to be considered. First, each portfolio aggregates over 600 firms. The SolarWinds breach might still be too financially localized to impact such a large number of firms, and the effect could be diluted among unaffected firms (those not associated with SolarWinds or not perceived by the market as affected). Second, none of the variations are statistically significant, and the overall impact of the event is likely mitigated by opposing behaviors. For instance, during the shock, investors might have shifted their investments to other stocks considered safe but still related to cybersecurity, or the event might have increased interest in cybersecurity and boosted investment in P5 firms.

Finally, I display in Tables 5.29 and 5.30 the cumulative abnormal returns of P20 and P5 but constructed with different cyber scores. There is not enough statistical significance to infer anything. Note that the cumulative returns still reach higher returns in the P20 case (figure 5.19) than in the P5 case (Figure 5.20), and the portfolios based on the various cyber scores seem to behave similarly which support the hypothesis that the market perceives a single aggregated risk related to cybersecurity.

These results contrast those of Florackis et al. (2023), who find a statistically significant drop in their top cyber-based portfolio returns around the event.

	CAR[-1,1]	CAR[-1,3]
overall	0.078	0.055
	[0.151]	[0.138]
preparation and reconnaissance	0.036	0.146
	[0.082]	[0.429]
persistence and evasion	0.163	0.228
	[0.301]	[0.543]
credential movement	0.141	0.312
	[0.255]	[0.724]
command and data manipulation	0.207	0.227
	[0.427]	[0.603]

Table 5.29: **Cumulative abnormal returns of cyber-based P20**

To estimate the cumulative abnormal returns (CAR), I use the market model around December 14, 2020, as $t = 0$. The beta of the market model is set up thanks to the returns of the prior year. The abnormal returns are given in percent. The t-statistics associated with the abnormal returns are given in the parenthesis.

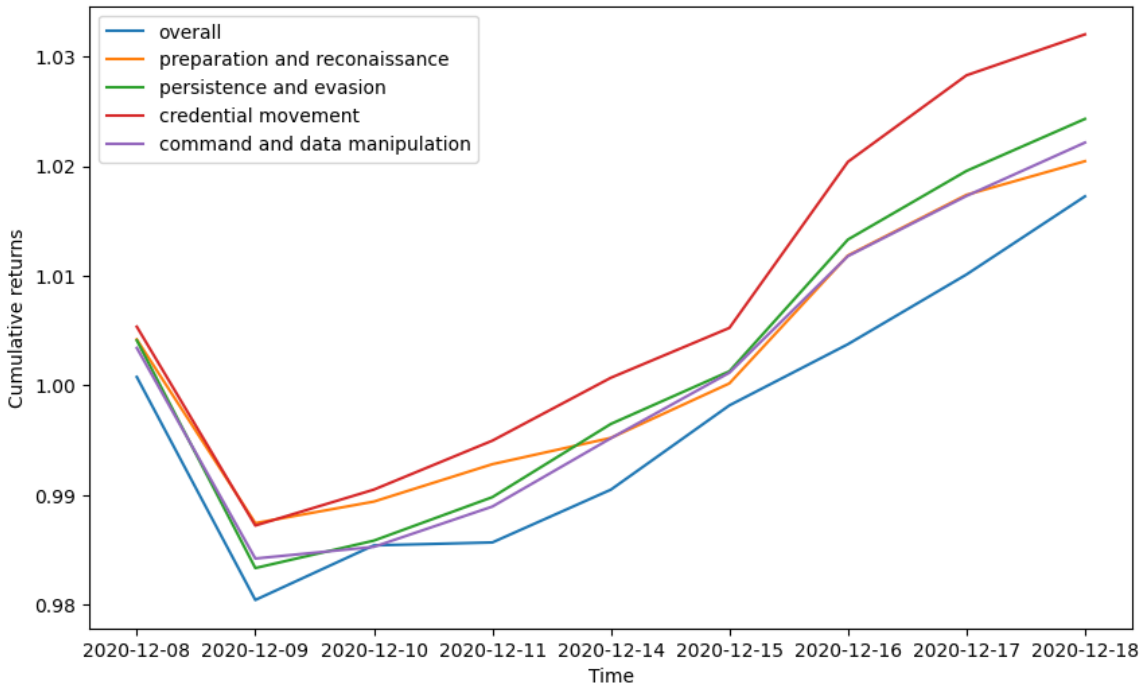

Figure 5.19: **Cumulative returns of cyber-based portfolio (P20) around SolarWinds breach**

	CAR[-1,1]	CAR[-1,3]
overall	0.206	0.194
	[0.616]	[0.748]
preparation and reconnaissance	0.182	0.181
	[0.639]	[0.818]
persistence and evasion	0.192	0.189
	[0.533]	[0.675]
credential movement	0.198	0.200
	[0.565]	[0.735]
command and data manipulation	0.009	0.081
	[0.029]	[0.336]

Table 5.30: **Cumulative abnormal returns of cyber-based P5**

To estimate the cumulative abnormal returns (CAR), I use the market model around December 14, 2020, as $t = 0$. The beta of the market model is set up thanks to the returns of the prior year. The abnormal returns are given in percent. The t-statistics associated with the abnormal returns are given in the parenthesis.

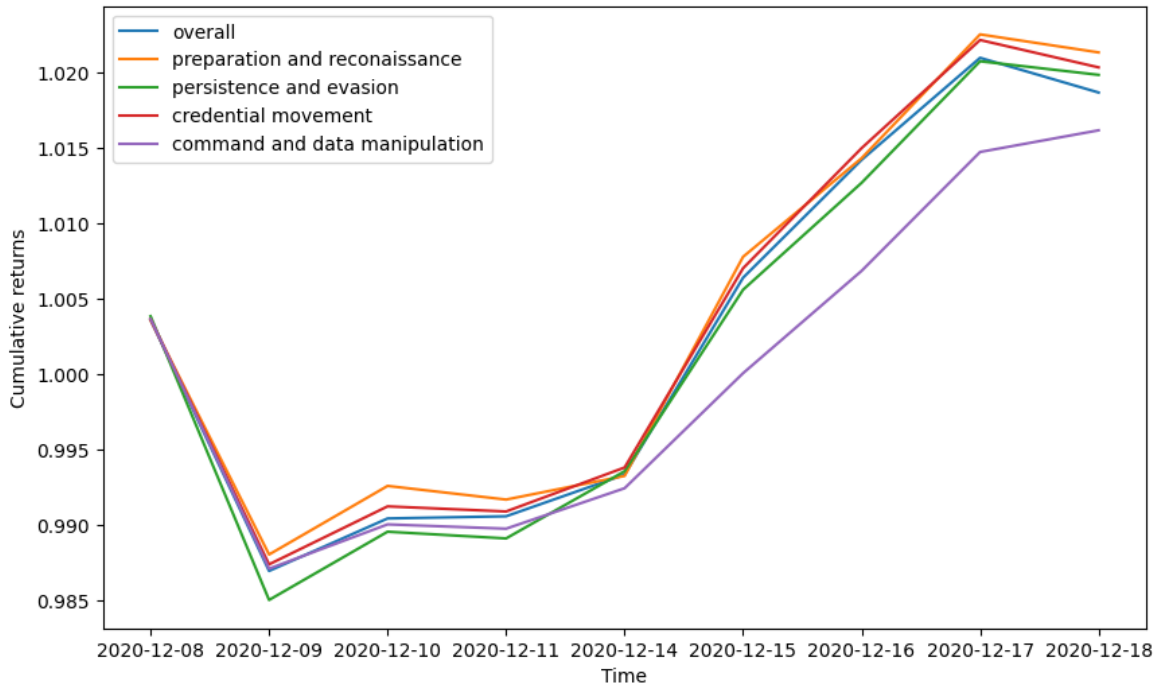

Figure 5.20: **Cumulative returns of cyber-based portfolio (P5) around SolarWinds breach**

Chapter 6

Conclusion

6.1 Conclusion

In this thesis, I use a doc2vec model to transform paragraphs of the MITRE ATT&CK database's descriptions of cyber attacks into vectors. Comparing those vectors based on their cosine similarity, I apply clustering methods such as K-means, Louvain, and spectral clustering to infer groups of cyber attacks belonging to four defined types (super-tactics): command and data manipulation, credential movement, persistence and evasion and preparation and reconnaissance. Those clusters were recurrent through different trials using the three methods and different hyperparameters. They were also chosen to preserve the underlying written structures of MITRE ATT&CK by using a two-score system that ensures the equal distribution of paragraphs across super-tactics and their exclusivity to these super-tactics.

Then, I use the doc2vec model to transform paragraphs of annual statements, more precisely 10-Ks, into vectors. Building the cosine similarity between 10-K vectors and vectors belonging to specific super tactics allows me to infer the semantic similarity of the 10-Ks to the four types of cyber attacks. I define those cosine similarities as the cyber score of a 10-K for a given super tactic. I also build an additional cyber sentiment score. This score considers only paragraphs' cyber scores when they contain words related to a "risk" or "uncertainty" vocabulary.

I find that the different cyber scores cannot be unexplained by the linear combination of standard financial variables and non-semantic variables of the firms they belong to (the highest R^2 within among all tested cyber scores is 0.43). The independence of those newly found variables supports their innovative nature. All aggregate cyber scores have increased over the years and are higher in industry sectors (from the 12 Fama-French industries classification) involving assisting and workflow-related technology like Telephone and Television Transmission or Business Equipment.

I conduct asset pricing and statistical tests involving portfolios sorted on firms' cyber scores to assess if the cyber scores reflect cyber risks. Since all results for each cyber score are similar to the overall cyber score and the previous study Celeny and Maréchal (2023) only used this undisentangled cyber score, I report here only the results related to this score. This does not apply to the cyber sentiment score, for which it appeared clear that no risk premium was involved.

Organizing firms into portfolios based on their cyber scores allows for the observation of increasing average excess returns as the portfolio's cyber score increases. The portfolio with the lowest quintile of cyber score, P1, has an average excess return of 0.82%. The portfolio with the highest quintile of cyber score, P5, has an average excess return of 1.44% (both statistically significant at the 1% level). Thus, a long-short portfolio P5-P1 destroys performance. Then, controlling for common pricing factors, I find that P5 has an alpha of 0.29% at the 1% level. Conversely, other portfolios, P1 to P4, have increasing alphas but are statistically insignificant. This threshold in significance between P4 and P5 highlights the fact that I cannot tell from a firm's cyber score, at which point it truly highlights cyber security in its 10-Ks. Therefore, lower portfolios contain a variety of firms that may be classified according to noise without meaning. I recommend that future studies using a similar work frame focus solely on P5 instead of P5-P1, as has been done until now. Sorting the firms into a first unrelated category and then according to their cyber score also reveals a similar structure of returns, as previously mentioned, with the top cyber-based portfolios performing better. Thus, the structure is robust, controlling for other firm characteristics.

Fama and MacBeth (1973) regressions show a risk premium associated with the cyber score and all disentangled cyber scores. In contrast, the cyber sentiment score does not drive any risk premium. The GRS test of Gibbons et al. (1989) shows that the long-short portfolio P5-P1 helps to price various assets when used with the other well-known pricing factors of the five-factor model Fama and French (2015). Furthermore, the BGRS tests from Barillas and Shanken (2018) also highlight that P5-P1 is an important cyber-based pricing factor. According to the test, this importance is rising with time. Interestingly, these observations are valid for all cyber scores, including the cyber sentiment score.

Last, I cannot reject the hypothesis that the return of P5-P1, built with different cyber scores, is statistically different. Then, I performed an event study using the cyber-breach of SolarWind in December 2020. The analysis provided no conclusive results, except that portfolios based on different cyber scores behave similarly. These last two observations could prove that the market does not differentiate between the various types of cyber risk and perceives them as a single aggregate cyber risk. This conclusion is reasonable when we observe the definition of the four types of cyber attacks. In a sense, they are not mutually exclusive since, in a cyber attack, command and data manipulation is the natural next step of credential movement, which is the next step of persistence, and evasion, which is the next step of preparation and reconnaissance.

6.2 Limitations

First, using disclosures like 10-Ks implicitly relies on the firms' willingness to disclose information about their cyber security. However, the SEC's new rule, effective July 26, 2023, requires companies to disclose significant cybersecurity incidents within four business days on Form 8-K and provide annual updates on their cybersecurity risk management and strategy in Form 10-K. Therefore my approach could significantly improve in the following years. Furthermore, on July 19, 2024, cybersecurity company CrowdStrike released a faulty update for one of its security software, causing around 8.5 million Microsoft Windows computers to crash and fail to restart

correctly. This incident touched many firms and could be a better cyber-related event to study in my framework.

Second, selecting the optimal neural network model for encoding paragraphs into vectors presents a challenge not addressed in Celeny and Maréchal (2023). In their study, various doc2vec models were trained by varying hyperparameters and using MITRE ATT&CK data and 10-Ks from 2007. The model that achieved the highest cyber score when applied to randomly selected firms' 10-K filings from 2008 was chosen. However, it could be argued that in 2008, firms had little incentive to disclose cybersecurity information in their 10-K filings or were not even concerned by cybersecurity, making these documents an unreliable metric for determining the best model. Conversely, using 10-K filings from recent years might introduce forward-looking biases that the authors likely aimed to avoid. Although one might argue that neural network encoding of paragraphs into vectors cannot incorporate future pricing information, this discussion is beyond the scope of my work. Another potential solution could be to use more recent 10-K filings, excluding data from before the year of the 10-Ks. However, the available dataset for this study was already relatively limited by general standards, and further reduction would be problematic.

Third, my approach cannot distinguish between companies that merely discuss cybersecurity because of its inherent risks and those that provide cybersecurity solutions. Nevertheless, the number of firms focusing exclusively on delivering cybersecurity solutions is relatively low. Celeny and Maréchal (2023) addressed this issue by conducting a robustness test to account for it and discard this potential issue.

6.3 Extension

The cyber sentiment score could be improved. I prioritized simplicity over precision, which affected its effectiveness. One potential enhancement would be to consider the cyber sentiment score when analyzing sentences containing words related to risk or uncertainty, including those in adjacent sentences or even further out. Another approach could involve developing a function that decreases as we move away from the risk-related sentence coupled with the cyber score to grant the cyber sentiment score. Furthermore, this research could greatly benefit from establishing a threshold for the cyber score that effectively distinguishes between relevant cyber-related and unrelated "noise" paragraphs.

The event analysis was conducted on portfolios comprising more than 600 firms, which leads to somewhat dubious conclusions. The analysis could be improved by examining firms individually during a cyber event rather than at an aggregate level. Comparing the cyber score levels and the average returns before and during the cyber event could provide additional evidence regarding the effectiveness of my assessment. I assume that Florackis et al. (2023) conduct their cyber-event analysis firm-wise leading to far higher statistical significance and better inference on the consequences of the event of December 2020 on the firms.

The cyber score evolves annually for a given firm and needs to be improved for effective comparison with market trends. To do so, I could increase the frequency of updates by incorporating information from 8-K filings and earnings calls. Other resources are also available for estab-

lishing a cyber score based on firms' technical data. I could compare these scores with the score produced by my semantical method to assess its performance.

Finally, these methods could be applied across various contexts, providing the existence of a relevant database similar in structure to MITRE ATT&CK. For instance, it could identify and discriminate across legislative, political, and environmental risks firms face, among other factors. The subsequent analysis to determine whether the score produced by this method reflects a risk is straightforward, with each step thoroughly detailed in this work.

Bibliography

Adosoglou, G., Lombardo, G., Pardalos, P. M., 2021. Neural network embeddings on corporate annual filings for portfolio selection. Expert Systems with Applications 164, 114053.

Antweiler, W., Frank, M. Z., 2004. Is all that talk just noise? The information content of internet stock message boards. Journal of Finance 59, 1259–1294.

Arslan-Ayaydin, O., Boudt, K., Thewissen, J., 2016. Managers set the tone: Equity incentives and the tone of earnings press releases. Journal of Banking and Finance 72, 132–147.

Barillas, F., Shanken, J., 2018. Comparing asset pricing models. Journal of Finance 73, 715–754.

Blondel, V. D., Guillaume, J.-L., Lambiotte, R., Lefebvre, E., 2008. Fast unfolding of communities in large networks. Journal of Statistical Mechanics: Theory and Experiment p. P10008.

Bodnaruk, A., Loughran, T., McDonald, B., 2015. Using 10-K text to gauge financial constraints. Journal of Financial and Quantitative Analysis 50, 623–646.

Calomiris, C. W., Mamaysky, H., 2019. How news and its context drive risk and returns around the world. Journal of Financial Economics 133, 299–336.

Carhart, M., 1997. On persistence in mutual fund performance. Journal of Finance 52, 57–82.

Celeny, D., Maréchal, L., 2023. Cyber risk and the cross section of stock returns. Available at http://dx.doi.org/10.2139/ssrn.4587993

Cochrane, J. H., 2005. The risk and return of venture capital. Journal of Financial Economics 75, 3–52.

Curiskis, S. A., Drake, B., Osborn, T. R., Kennedy, P. J., 2020. An evaluation of document clustering and topic modelling in two online social networks: Twitter and Reddit. Information Processing and Management 57 (2), 102034.

Fama, E. F., French, K. R., 1992. The cross-section of expected stock returns. Journal of Finance 47, 427–465.

Fama, E. F., French, K. R., 2015. A five-factor asset pricing model. Journal of Financial Economics 116, 1–22.

Fama, E. F., MacBeth, J. D., 1973. Risk, return, and equilibrium: Empirical tests. Journal of Political Economy 81, 607–636.

Feldman, R., Govindaraj, S., Livnat, J., Segal, B., 2010. Management's tone change, post earnings announcement drift and accruals. Review of Accounting Studies 15, 915–953.

Florackis, C., Louca, C., Michaely, R., Weber, M., 2023. Cybersecurity risk. Review of Financial Studies 36, 351–407.

Garcia, D., 2013. Sentiment during recessions. Journal of Finance 68, 1267–1300.

Gibbons, M. R., Ross, S. A., Shanken, J., 1989. A test of the efficiency of a given portfolio. Econometrica 57, 1121–1152.

Gomes, O., Mihet, R., Risbabh, K., 2023. Data risk, firm growth and innovation. Available at: http://dx.doi.org/10.2139/ssrn.4559921

Harvey, C. R., Liu, Y., Zhu, H., 2016. ...and the cross-section of expected returns. Review of Financial Studies 29, 5–68.

Hassan, T. A., Hollander, S., van Lent, L., Tahoun, A., 2019. Firm-level political risk: Measurement and effects. Quarterly Journal of Economics 134, 2135–2202.

Jamilov, R., Rey, H., Tahoun, A., 2023. The anatomy of cyber risk. Available at: https://ssrn.com/abstract=3866338

Jegadeesh, N., Wu, D., 2013. Word power: A new approach for content analysis. Journal of Financial Economics 110, 712–729.

King, G., Lam, P., Roberts, M. E., 2017. Computer-assisted keyword and document set discovery from unstructured text. American Journal of Politcal Science 61, 971–988.

Lau, J. H., Baldwin, T., 2016. An empirical evaluation of doc2vec with practical insights into document embedding generation. In: *Proceedings of the 1st Workshop on Representation Learning for NLP*, Association for Computational Linguistics, Berlin, Germany, pp. 78–86.

Le, Q., Mikolov, T., 2014. Distributed representations of sentences and documents. In: Xing, E. P., Jebara, T. (eds.), *Proceedings of the 31st International Conference on Machine Learning*, PMLR, Bejing, China, pp. 1188–1196.

Lintner, J., 1965. The valuation of risk assets and the selection of risky investments in stock portfolios and capital budgets. Review of Economics and Statistics 47, 13–37.

Liu, J., Marsh, I. W., Xiao, Y., 2022. Cybercrime and the cross-section of equity returns. Avaiable at: http://dx.doi.org/10.2139/ssrn.4299599

Mikolov, T., Chen, K., Corrado, G., Dean, J., 2013. Efficient estimation of word representations in vector space.

Mossin, J., 1966. Equilibrium in a capital asset market. Econometrica 34, 768–783.

Ross, S. A., 1976. The arbitrage theory of capital asset pricing. Journal of Economic Theory 13, 341–360.

Sautner, Z., van Lent, L., Vilkov, G., Zhang, R., 2023. Firm-level climate change exposure. Journal of Finance 78, 1449–1498.

Sharpe, W. F., 1964. Capital asset prices: A theory of market equilibrium under conditions of risk. Journal of Finance 19, 425–442.

Treynor, J. L., 1962. Toward a theory of market value of risky assets. Available at: http://dx.doi.org/10.2139/ssrn.628187

Appendix

Variable	Description	Source
Firm size (ln)	ln(total assets [at])	Compustat
Firm Age (ln)	ln(years) since the firm first appeared in Compustat	Compustat
Book to market ratio	Common equity [ceq] / market equity [prc*shrout]	Compustat and CRSP
Tobin's Q	(Total assets - common equity + market equity) / total assets	Compustat and CRSP
ROA	Net income [ni] / total assets	Compustat
Market Beta	5-year rolling market beta [beta]	Compustat
Intangible/Assets	Intangible assets [intan] / total assets	Compustat
Debt/assets	Total Debt / Total Assets [debt_assets]	WRDS Financial Ratios
ROE	Net Income / Book Equity [roe]	WRDS Financial Ratios
Price/Earnings	Stock Price / Earnings [pe_exi]	WRDS Financial Ratios
Profit Margin	Gross Profit / Sales [gpm]	WRDS Financial Ratios
Asset Turnover	Sales / Total Assets [at_turn]	WRDS Financial Ratios
Cash Ratio	(Cash + Short-term Investments) / Current Liabilities [cash_ratio]	WRDS Financial Ratios
Sales/Invested Capital	Sales per dollar of Invested Capital [sale_invcap]	WRDS Financial Ratios
Capitalization Ratio	Long-term Debt / (Long-term Debt + Equity) [capital_ratio]	WRDS Financial Ratios
R&D/Sales	R&D expenses / Sales [RD_SALE]	WRDS Financial Ratios
ROCE	Earnings Before Interest and Taxes / average Capital Employed [roce]	WRDS Financial Ratios
Readability (ln)	Number of characters in the 10-K	EDGAR - SEC
Risk section length (ln)	Number of sentences in Item 1A of the 10-K	EDGAR - SEC
Secrets	As defined in Florackis et al. (2023)	EDGAR - SEC
Volume per capital	Monthly trading volume / Market capitalization	CRSP
Humans per capital	Monthly number of employees / Market capitalization	Compustat and CRSP

Table A.1: **Variable definitions**

This table reports the variable names used throughout the paper, their description, and their source. Square brackets indicate variable name definitions in CRSP and Compustat.

Risk/Uncertainty dictionary : risk, jeopardize, riskiness, risks, unsettled, treacherous, uncertainty, unpredictability, oscillating, variable, dilemma, perilous, chance, skepticism, tentativeness, possibility, hesitancy, unreliability, pending, riskier, wariness, uncertainties, unresolved, vagueness, uncertain, unsure, dodgy, doubt, irregular, equivocation, prospect, jeopardy, indecisive, bet, suspicion, chancy, variability, risking, menace, exposed, peril, qualm, likelihood, hesitating, vacillating, threat, risked, gnarly, probability, unreliable, disquiet, unknown, unsafe, ambivalence, varying, hazy, imperil, unclear, apprehension, vacillation, unpredictable, unforeseeable, incalculable, speculative, halting, untrustworthy, fear, wager, equivocating, reservation, torn, diffident, hesitant, precarious, fickleness, gamble, undetermined, misgiving, risky, insecurity, changeability, instability, debatable, undependable, doubtful, undecided, incertitude, hazard, dicey, fitful, tricky, indecision, parlous, sticky, wavering, unconfident, dangerous, iffy, defenseless, tentative, faltering, unsureness, hazardous, endanger, fluctuant, queries, quandary, niggle, danger, insecure, diffidence, fluctuating, changeable, precariousness, unstable, riskiest, doubtfulness, vague, hairy, erratic, ambivalent, query, dubious (Hassan et al., 2019)

Cyber score	**Covariance** $\cdot 10^3$	**Correlation**
persistence	0.2777	0.1038
command and control	0.3146	0.1281
impact	0.2960	0.1079
initial access	0.2237	0.0766
resource development	0.1841	0.0629
collection	0.2035	0.0723
exfiltration	0.1473	0.0499
credential access	0.2515	0.0916
privilege escalation	0.3088	0.1286
execution	0.2704	0.1121
defense evasion	0.1809	0.0761
reconnaissance	0.2145	0.0768
lateral movement	0.1272	0.0488
discovery	0.1640	0.0681
preparation and reconnaissance	0.1958	0.0710
persistence and evasion	0.1914	0.0795
credential movement	0.2350	0.0867
command and data manipulation	0.2114	0.0756
overall	0.1799	0.0699
sentiment	-0.0408	-0.0095

Table A.2: **Cyber scores correlation and covariance with idiosyncratic volatility**

Correlation and covariance of the different cyber scores with the idiosyncratic volatility of the firms they are associated with. The idiosyncratic volatility at a given time is computed as the root squared of $var(\epsilon_i) = var(r_i) - cov(r_i, r_m)^2/var(r_m)$ taken over the last five years, where r_i and r_m are the excess return of the firm and the market. The covariance is multiplied by 10^3 to improve readability.