mathematics

MDPI

Article

Quantifying Cybersecurity Impacts on Clean Energy Market Volatility: A Time-Frequency Approach

Catalin Gheorghe and Oana Panazan *

Department of Engineering and Industrial Management, Transilvania University of Brasov, Eroilor Street 29, 500036 Brasov, Romania; gheorghe.c@unitbv.ro

* Correspondence: oana.panazan@unitbv.ro

Abstract: This study investigates the impact of cyber threats on the clean energy (CE) market, which is increasingly dependent on digital technologies and interconnected infrastructure. The sector's growing digitalization makes it more susceptible to cyberattacks, leading to significant effects on market volatility and financial performance. Using time-varying parameter vector autoregression (TVP-VAR), wavelet coherence models, and rolling window analysis, this research examines the dynamic relationships between cyberattacks and the CE market over various timescales. The severity of cyberattacks is quantified using the OWASP risk rating methodology, providing a structured approach to assessing cyber risks. The findings reveal that high-severity cyberattacks targeting critical infrastructures generate pronounced short-term volatility, especially in concentrated indices such as TAN and ICLN. In contrast, diversified indices like PBW and RNRG demonstrate greater resilience, highlighting the protective role of portfolio diversification. Moreover, the impact of cyber threats is exacerbated during periods of macroeconomic instability, reinforcing the need for integrated risk management approaches. These results provide actionable insights for investors and policymakers, emphasizing the need for proactive risk management strategies to enhance market resilience and safeguard the CE sector from cybersecurity threats.

Keywords: cybersecurity; attack; clean energy; volatility; wavelet

MSC: 91G70; 90B50; 62P05

Academic Editor: Anatoliy Swishchuk

Received: 28 March 2025
Revised: 11 April 2025
Accepted: 15 April 2025
Published: 17 April 2025

Citation: Gheorghe, C.; Panazan, O. Quantifying Cybersecurity Impacts on Clean Energy Market Volatility: A Time-Frequency Approach. *Mathematics* **2025**, *13*, 1320. https://doi.org/10.3390/math13081320

1. Introduction

Cyber risks have become significant drivers of financial market volatility, particularly in digital-intensive sectors like technology and CE. The increasing digitalization of the CE sector enhances operational efficiency while introducing substantial vulnerabilities. Cyberattacks are acute risks that exploit the interconnectedness of digital infrastructures, creating systemic disruptions that can destabilize markets [1,2]. These risks are magnified by the complexity of global events like the COVID-19 pandemic and geopolitical conflicts, such as the war in Ukraine, highlighting the fragility of critical infrastructures [3]. A sectoral approach to cyber resilience is required to address these challenges, emphasizing the mitigation of feedback loops, supply chain vulnerabilities, and systemic interdependencies [4]. Furthermore, market reactions to cyber risks may be compounded by broader factors such as investor sentiment [5], political uncertainty [6], and

macroeconomic instability—including inflation, interest rate shocks, and exchange rate volatility [7,8].

Empirical evidence supports the critical role of cyber risks in amplifying financial volatility, particularly in digitalized sectors. For instance, Akyildirim et al. [9] and Tosun [10] found that cyberattacks result in abrupt price fluctuations, especially in technology and energy-related stocks. Events such as the Colonial Pipeline ransomware attack in 2021 led to significant disruptions in energy markets and heightened risk premiums [11]. These findings support the inclusion of cyber risks in portfolio diversification strategies, given their potential to undermine traditional risk mitigation approaches.

The financial implications of cyberattacks on CE markets remain underexplored, despite the growing reliance of the sector on digital connectivity. According to the International Monetary Fund [12], nearly 20% of cyber incidents over the past decade have targeted the financial sector, underscoring the widespread impact of these risks. The International Energy Agency [13] highlights the unique susceptibility of CE markets due to their dependence on digital infrastructure. Cyber incidents affecting energy assets, trading platforms, or financial intermediaries linked to CE investments can trigger price instability, increase risk premium, and create uncertainty in capital flows.

The financial impact of cyberattacks on CE markets occurs through multiple transmission channels. Operational disruptions caused by attacks on energy firms can directly affect electricity supply and pricing, leading to immediate volatility. Data breaches or manipulation of energy trading platforms reduce investor confidence, causing capital flight and amplifying systemic risk. Cyberattacks targeting supply chain components within the CE sector create additional uncertainty, particularly when disruptions affect key production or distribution networks. The interconnected nature of CE firms means that cyber incidents can have cascading effects across the entire sector, amplifying financial instability [14].

Existing research on CE market volatility has focused predominantly on conventional financial risks, such as oil price fluctuations [15], geopolitical risks [16], and the influence of CE investments [17]. While these factors drive market fluctuations through relatively predictable mechanisms, cyber risks generate abrupt exogenous shocks that require new analytical approaches to measure their impact. Cyber incidents introduce informational asymmetries that heighten speculation and volatility, as market participants react to uncertainty regarding the extent and consequences of an attack. Regulatory responses, including stricter compliance measures or government intervention following major cyberattacks, can further influence CE asset pricing and financial market stability.

The theoretical foundation of this analysis can be traced to asset pricing theory and modern portfolio theory [18], which emphasize the role of diversification in reducing unsystematic risk. However, cyberattacks may generate systemic shocks that limit the effectiveness of diversification strategies. Signal theory further explains how cyber incidents transmit negative information to investors, affecting expectations and asset valuations [19]. Additionally, the efficient market hypothesis suggests that markets incorporate new information rapidly, yet cyber threats may cause deviations from rational pricing due to information asymmetry and uncertainty [20]. Together, these theoretical perspectives clarify the mechanisms through which cybersecurity incidents affect volatility, returns, and portfolio construction.

Despite increased scholarly interest in technological disruptions, the intersection between cybersecurity and CE finance remains underexplored. This study addresses these gaps by analyzing how cyber risks impact CE financial indices and exchange-traded funds (ETFs) across different time horizons, employing a novel methodological framework that combines TVP-VAR, wavelet coherence analysis, and rolling windows. TVP-VAR enables the identification of evolving relationships between cyber risk exposure and market

reactions, revealing periods when financial markets are most sensitive to cyber threats. Wavelet analysis provides time-frequency decomposition, offering granular insights into short-term and long-term market responses. The use of rolling windows allows for the detection of time-varying dynamics, capturing structural shifts. These methodologies allow for a comprehensive evaluation of cyber risk dynamics in CE markets [21].

This research further integrates the Open Web Application Security Project (OWASP) [22] framework to measure the severity of cyberattacks. OWASP quantifies attacks by assessing their impact on confidentiality, integrity, and availability, enabling the transformation of qualitative cyber risk data into structured numerical metrics. By incorporating these metrics into econometric analysis, the study bridges the gap between cybersecurity risk assessment models and financial market analysis, allowing for a more precise estimation of how cyberattack frequency, intensity, and targeting drive market volatility.

While prior studies have explored clean energy volatility through the lens of oil markets, ESG policies, and green asset pricing [16,17,23], this research is the first to quantitatively integrate OWASP-based cybersecurity metrics into advanced econometric modeling. By examining sector-specific differences between concentrated (e.g., ICLN, TAN) and diversified (e.g., PBW, RNRG) CE indices, it provides new insights into the financial implications of cyber risk exposure and resilience.

The study's contribution is threefold. First, it dynamically evaluates the financial implications of cyber risks, capturing both short-term and long-term effects. Second, it introduces a novel integration of cybersecurity metrics with financial modeling, leveraging OWASP's standardized framework within an econometric structure. Third, it provides actionable insights for investors, policymakers, and portfolio managers, highlighting strategies such as diversification and proactive cybersecurity investments to enhance market resilience. To our knowledge, this study is the first to examine the dynamic effects of cyberattack characteristics on CE financial markets, offering an innovative approach to understanding the intersection of digital security and financial stability [24].

The remainder of this paper is structured as follows. Section 2 reviews the relevant literature on cyber risks and financial market volatility, providing the conceptual foundation for this study. Section 3 outlines the methodological framework, detailing the econometric models and the OWASP-based risk evaluation approach. Section 4 presents the empirical findings, emphasizing both temporal and frequency-specific effects of cyber risks on CE markets. Section 5 discusses the theoretical and practical implications of the results, while Section 6 concludes with key insights and recommendations for future research.

2. Literature Review

2.1. Cybersecurity Risks and Financial Market Implications in the CE Sector

The increasing digitalization of the CE sector has enhanced operational efficiency but has also heightened exposure to cyber risks, leading to significant financial consequences. CE markets rely heavily on smart grids, blockchain-based energy trading platforms, and IoT-enabled infrastructure, which, despite their benefits, introduce systemic vulnerabilities that amplify financial instability [25]. Blockchain applications, for example, require robust security measures to prevent manipulation of energy trading transactions [26], while IoT-based smart grids improve energy efficiency but expand the attack surface for potential cyber threats [17].

These vulnerabilities impact CE markets in several ways. First, cyberattacks targeting energy firms or infrastructure create operational disruptions that can lead to supply chain instability and energy price volatility. Second, financial instruments linked to the CE sector, such as ETFs and stock indices, are directly affected by shifts in investor sentiment, which reacts to informational asymmetry and regulatory uncertainty following cyber

incidents [27]. The increasing sophistication of cyber threats further complicates financial stability, as highlighted by Mitra et al. [28], who noted the challenges of securing large-scale digital infrastructures in the face of evolving cyber threats.

Despite efforts to enhance cybersecurity frameworks, including the adoption of regulatory standards and risk management protocols, market-wide disruptions from cyber incidents persist. Arfaoui et al. [23] suggest that diversified investment portfolios may help mitigate market volatility, while studies by Hu et al. [29] highlight the role of public–private partnerships in strengthening critical infrastructure resilience. However, existing research has largely overlooked the role of cyber risks in shaping CE financial markets across different time horizons, an aspect this study addresses by analyzing both short-term and long-term financial impacts of cyber threats on CE indices.

2.2. Cyber Risks as Drivers of Market Volatility

Cyber risks have been increasingly recognized as systemic threats to financial stability, particularly in industries that depend on digital infrastructure. Unlike traditional financial risks, cyber threats generate exogenous shocks, disrupting markets without warning and amplifying speculative volatility [7,30]. The CE sector is particularly exposed to such risks due to its reliance on decentralized networks and digital asset trading platforms.

Empirical research highlights the market-wide impact of cyber incidents. Akyildirim et al. [9] found that stock prices of affected companies decline by an average of 0.24% immediately following a cyberattack, with recovery often taking up to two weeks. Lucey and Ren [31] identified that green stocks exhibit heightened sensitivity to cybersecurity risks, while green bonds act as partial risk hedges in volatile periods [32]. These findings suggest that the financial reaction to cyber threats is not uniform across asset classes, emphasizing the need for a differentiated analysis of cyber risk transmission channels in CE markets.

Emerging markets face additional risks due to limited investment in cybersecurity infrastructure. Ding et al. [8] found that cyber risk spillovers between energy and commodity markets contribute to financial instability, while Tosun [10] demonstrated that cyberattacks trigger increased trading volumes and sharp investor reactions, leading to long-term investment reductions.

Although these studies provide valuable insights, the literature lacks a detailed examination of how cyber risks dynamically influence CE financial indices and ETFs. This study fills this gap by integrating advanced econometric methodologies to capture the time-varying and frequency-specific effects of cyber incidents on CE financial markets [33].

2.3. Financial Market Reactions to Cyberattacks in the CE Sector

The impact of cyberattacks on CE financial markets remains insufficiently explored, despite growing evidence of their destabilizing effects on investor confidence and market volatility. Attacks targeting CE firms, digital energy trading platforms, and infrastructure components can lead to cascading financial disruptions, affecting stock price trends and investment flows. Boakye et al. [33] identified that cyber incidents in microgrid networks create systemic contagion effects, disrupting both energy and financial markets.

Certain financial instruments, such as carbon credit futures, have been proposed as potential hedging tools against cyber-induced volatility, but their effectiveness remains limited during major financial crises [34]. The unpredictability of cyber threats further complicates financial risk management, as they introduce nonlinear spillover effects that traditional models struggle to capture.

To analyze the financial transmission of cyber risks, this study employs a novel econometric framework that integrates cybersecurity risk assessment models into financial analysis. This includes the use of TVP-VAR models, which are well-suited to detecting time-varying interdependencies and evolving dynamics, and wavelet coherence analysis, which captures short- and long-term market reactions across frequencies. Lucey and Ren [31] demonstrated the value of TVP-VAR in identifying indirect financial dependencies, while Husain et al. [34] validated wavelet analysis as a robust tool for measuring time-frequency interactions between financial shocks and cyber incidents. Building on this foundation, this study extends the analysis by incorporating OWASP-based cyber risk severity scores. Although OWASP was developed for application-level risk evaluation, its structured and quantifiable scoring system provides a bridge between cybersecurity assessments and macro-financial analysis, enhancing the precision and interpretability of econometric modeling in CE financial markets.

3. Data and Methodology

This study investigates how cyberattacks affect both CE stock indices and ETFs, employing attack-specific variables alongside advanced econometric and time-series analysis methods to capture the dynamic relationships over time. Figure 1 presents the conceptual framework, illustrating the relationships between variables.

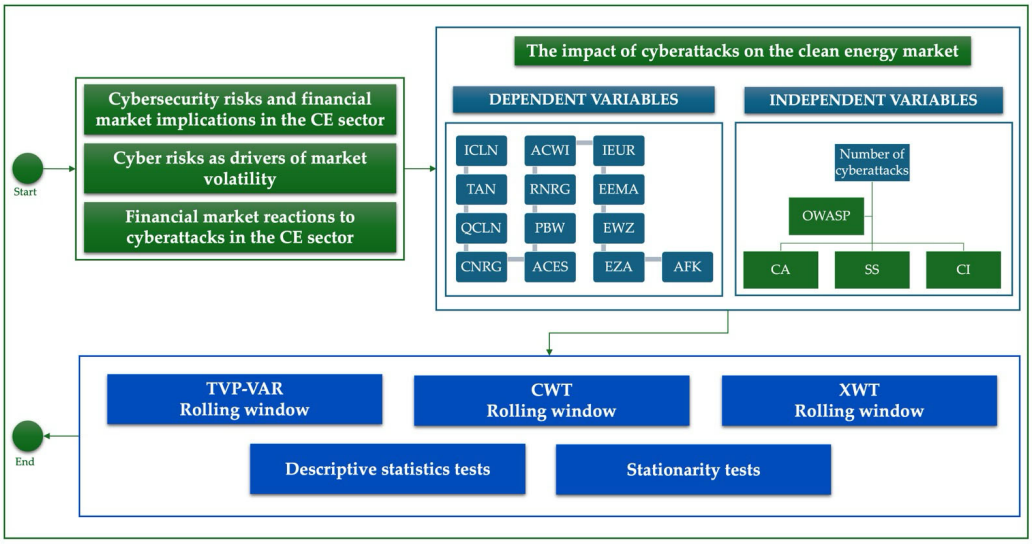


Figure 1. Conceptual framework. Source: Own elaboration.

3.1. Sample and Data

This study employs a dual approach by analyzing both stock indices and ETFs relevant to the CE market. This approach ensures that the findings are not overly dependent on a single market segment and minimizes the risk of overgeneralization.

The inclusion of ETFs in this study is justified by their ability to offer a comprehensive representation of the CE sector, as they encompass a broad range of companies involved in solar, wind, battery storage, and infrastructure technologies. Unlike individual stocks, which are more susceptible to firm-specific events, ETFs provide greater stability by reflecting aggregated market movements. Their widespread use in financial research further supports their relevance, as they serve as effective tools for assessing market trends and investor sentiment. By capturing the performance of multiple CE sub-sectors, ETFs offer a more reliable measure of systemic risk, particularly in the context of cyberattacks.

In parallel, stock indices serve as benchmarks for the overall CE market, offering insights into sector-wide trends and macroeconomic influences. The combined use of ETFs and stock indices in this study ensures a more comprehensive analysis by accounting for both market-wide effects and company-specific reactions to cyber risks. This dual approach strengthens the study's ability to capture the broader financial implications of cyber threats on CE investments.

The selected indices include the iShares Global CE Index, First Trust NASDAQ Clean Edge Green Energy ETF, and Invesco Wilder Hill CE ETF, which are prominent in the literature and frequently used in recent studies [7,35]. These indices provide comprehensive details on the CE sector, including solar and wind energy companies and infrastructure and technology providers. Similarly, ETFs like ICLN and TAN represent major players in the CE market and were included due to their frequent use in related research. For example, Yousaf et al. [36] analyzed the interaction between CE ETFs and green bonds, while Chatziantoniou et al. [16] used these ETFs to capture market trends while exploring the effects of sustainable investments and oil prices.

The analysis spans October 2018 (26 October 2018 CNRG listing date) to March 2025, capturing a recent surge in cyberattacks targeting CE infrastructure. Additionally, this period coincides with the sector's increasing reliance on interconnected digital technologies, amplifying the financial impact of cyberattacks. This study provides a timely analysis of the interplay between cyber risks and market volatility in a highly vulnerable sector by focusing on this timeframe.

Financial data for the indices were sourced from Investing.com [37]; data for the ICLN and TAN ETFs, including closing prices and trading volumes, were obtained from Yahoo Finance [38] and Bloomberg Terminal [39]. These platforms provide accurate financial data and align with the cyberattack series, creating a robust foundation for analyzing the relationship between cyber risks and market performance. The selected global indices and ETFs also enhance regional diversification, minimizing the influence of region-specific factors on the results.

Variables related to cyber risks were constructed using a day-of-occurrence time-series, capturing the number of reported attacks during the analysis period. Data were collected from public sources and specialized databases, including the Privacy Rights Clearinghouse [40], Hackmageddon [41], Eurepoc [42], and CSIS [43]. Each observation included details of attacks targeting critical infrastructure in the energy sector; severity and type were recorded where available. We calculated the severity scores using the OWASP methodology, integrating the probability of occurrence with the impact on system confidentiality, integrity, and availability.

3.2. Explanatory Variables

3.2.1. Dependent Variables

To assess the performance of the CE market, we selected several relevant stock indices that are representative of this sector. Table 1 presents the analyzed indices in detail.

Table 1. Variables description.

Category	Variable	Summary	Variable Type	Unit
Dependent	ICLN (iShares Global Clean Energy ETF)	Represents the performance of CE companies	Continuous	Closing price (USD/unit)
Dependent	TAN (Invesco Solar ETF)	Represents the achievements of companies in the solar sector	Continuous	Closing price (USD/unit)

Dependent	QCLN (First Trust NASDAQ Clean Edge Green Energy ETF)	Tracks companies in the CE sector, including solar and wind	Continuous	Closing price (USD/unit)
Dependent	CNRG (SPDR Kensho Clean Power ETF)	Focuses on innovative CE companies	Continuous	Closing price (USD/unit)
Dependent	ACES (ALPS Clean Energy ETF)	Contains low-carbon and renewable energy companies	Continuous	Closing price (USD/unit)
Dependent	PBW (Invesco Wilder Hill Clean Energy ETF)	Diversified index for CE, including green technologies	Continuous	Closing price (USD/unit)
Dependent	RNRG (Global X Renewable Energy Producers ETF)	Index for global renewable energy producers	Continuous	Closing price (USD/unit)
Dependent	ACWI (iShares MSCI ACWI ETF)	Diversified global index with exposure to developed and emerging markets	Continuous	Closing price (USD/unit)
Dependent	IEUR (iShares Core MSCI Europe ETF)	Index for developed markets in Europe	Continuous	Closing price (USD/unit)
Dependent	EEMA (iShares MSCI Emerging Markets Asia ETF)	Index for emerging markets in Asia	Continuous	Closing price (USD/unit)
Dependent	EWZ (iShares MSCI Brazil ETF)	Index focused on the Brazilian equity market	Continuous	Closing price (USD/unit)
Dependent	EZA (iShares MSCI South Africa ETF)	Index focused on the South African equity market	Continuous	Closing price (USD/unit)
Dependent	AFK (VanEck Africa Index ETF)	Diversified index for African markets	Continuous	Closing price (USD/unit)
Independent	Number of cyberattacks	The total frequency of cyberattacks recorded on the days of their occurrence	Continuous	Number
Independent	Severity of cyberattacks	Impact scores or descriptions that assess the severity of cyberattacks	Continuous	Number
Independent	Cyberattack Intensity	The ratio between the number of attacks on a given day and the maximum observed in the dataset.	Continuous	Number (value between 0 and 1)

Note: The table outlines the study's variables. Dependent variables represent CE ETFs' performance, and independent variables capture cyberattack frequency, type, and severity.

3.2.2. Independent Variables

The following independent variables were used to examine the influence of cyberattacks on CE stocks:

- Number of cyberattacks. This variable represents the daily frequency of reported cyberattacks during the analysis period.
- Severity of cyberattacks. This continuous variable was calculated using the OWASP methodology. The resulting numeric scores provide a detailed assessment of each attack's severity, allowing for a nuanced analysis of its potential to induce volatility in financial markets;
- Cyberattack intensity. The ratio between the number of attacks on a given day and the maximum number of attacks in the dataset, indicating the relative intensity of the attack on that day.

This study employs the OWASP Risk Rating Methodology to assess the severity of cyberattacks targeting the CE sector. While OWASP is primarily designed for evaluating web application security, its structured and standardized scoring approach can be adapted for macro-financial contexts. By translating cyber incidents into quantifiable risk metrics, OWASP allows integration into econometric models sensitive to risk asymmetries and tail events. To ensure consistency and reliability, the OWASP-based scoring system in this study follows a structured process that evaluates each reported cyberattack based on its impact on confidentiality, integrity, and availability. Confidentiality refers to the extent to which sensitive financial, operational, or energy infrastructure data are exposed or manipulated. Integrity captures the degree of alteration or corruption of critical system functions, including incidents such as energy price manipulation or disruptions affecting blockchain-based energy trading platforms. Availability assesses the effect of cyberattacks on system uptime, considering disruptions in smart grids, IoT-enabled monitoring systems, and digital trading mechanisms. This approach provides a comprehensive assessment of cyber risks by capturing their effects on different aspects of the CE sector's digital infrastructure.

To ensure distributional stability and enable integration within an autoregressive framework sensitive to outliers, a nonlinear monotonic transformation was applied to the observable variable CA. Accordingly, the severity score (SS) is defined as a composite entropic logarithmic function, commonly used in modeling rare phenomena characterized by heavy-tailed distributions.

$$SS_t = \phi(CA_t) \quad (1)$$

where ϕ is a sublinear, monotonic function with a positive and decreasing derivative, which intuitively compresses extreme cyberattack frequencies into a bounded risk intensity scale. This preserves the interpretability of outlier shocks and reduces their dominance over the system's dynamics [44,45].

To facilitate trans-temporal and inter-regional comparability, a unitary rescaling of the observable indicator was performed by applying a Lipschitz-continuous projection function within a higher-order normed space. Accordingly, the composite intensity index (CI) reflects the relative distribution of values with respect to the point of empirical saturation, preserving structural proportionality across entities with differing dynamics.

$$CI_t = \psi(CA_t) \quad (2)$$

where $\psi(CA_t) \in [0, 1]$ and $\sup \psi(CA_t) = 1$. Function ψ ensures comparability by mapping cyberattack frequencies onto a normalized scale, capturing systemic saturation and enabling alignment across datasets of different magnitudes [6].

Figure 2 shows a strong and dynamic relationship between the frequency of cyberattacks and the performance of CE ETFs, demonstrating the substantial influence of digital risks on prices and returns in the short and medium term. From 2020 to 2021, ETFs such as ICLN, TAN, and PBW proliferated, followed by periods of high volatility and pronounced declines. These trends reflect the sector's high sensitivity to external shocks, including cyberattacks and significant crises like the COVID-19 pandemic. The CE companies rely heavily on interconnected digital technologies, which compounds this vulnerability and exposes them to significant operational and financial risks.

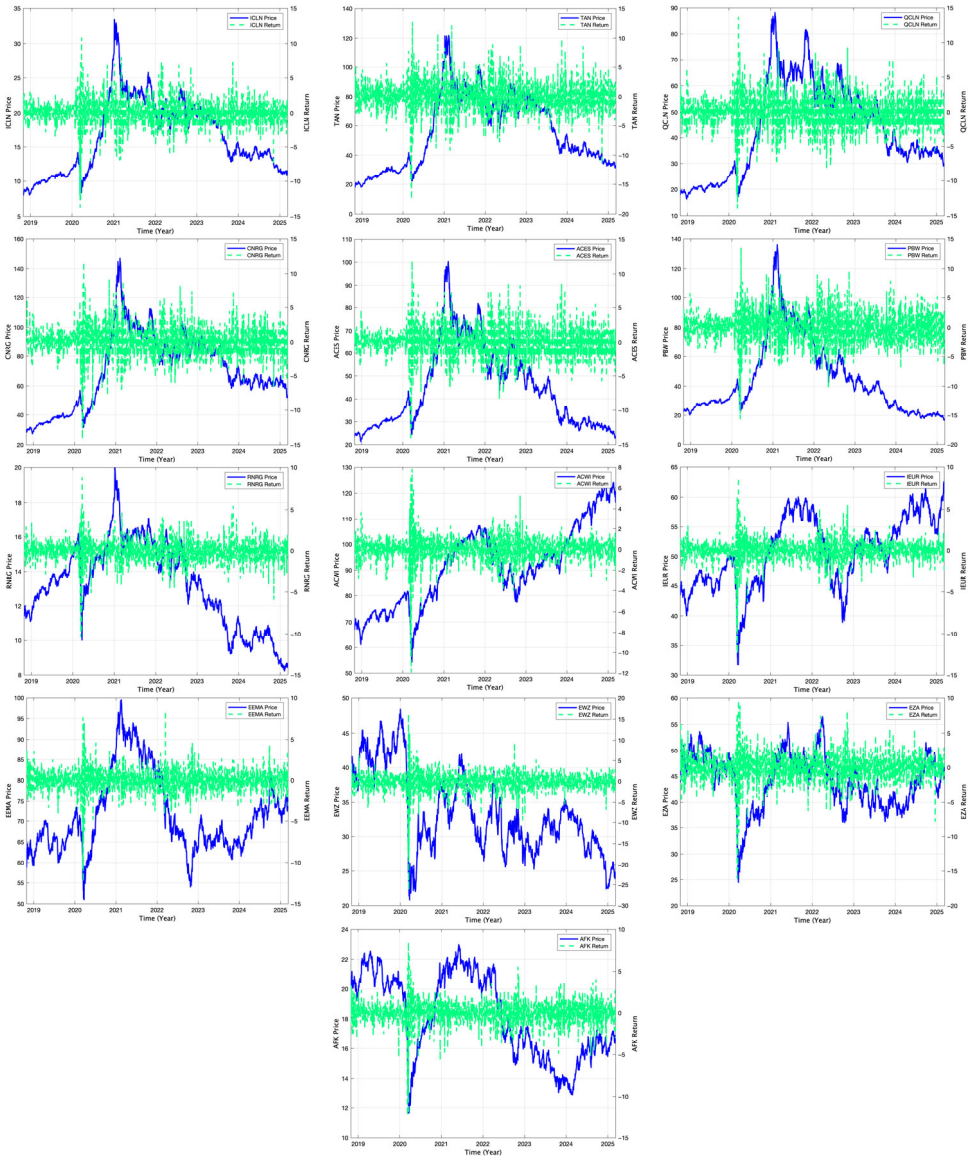


Figure 2. Evolution of prices and returns. Source: Own elaboration.

The long-term data (2023–2024) indicate a trend toward market stabilization, suggesting that increased investments in cybersecurity and enhanced organizational resilience have mitigated the impact of cyber risks. These findings emphasize the need to integrate cyber risk considerations into financial valuation models and investment strategies. The results also demonstrate the central role of cyberattacks in amplifying financial market volatility within the CE sector, providing a robust foundation for adopting proactive digital risk management practices to protect market stability and foster sustainable investment [46].

3.3. Analysis Methods

This study employs advanced time-series analysis methods to explore the relationship between cyberattacks and CE market performance. The central econometric tool is the TVP-VAR model, which allows for evolving interdependencies among variables. By estimating time-varying coefficients, this model facilitates the identification of temporal windows of increased market sensitivity to cyber risks. TVP-VAR has been effectively

used in prior studies to assess financial contagion and shock transmission in contexts characterized by instability and nonlinear spillovers [47,48].

The continuous wavelet transform (CWT) complements the TVP-VAR framework by providing a time-frequency perspective. CWT enables the decomposition of the co-movement into specific frequencies and periods, thus distinguishing between short-term reaction patterns and long-term structural shifts in market dynamics.

Additionally, the cross-wavelet transform (XWT) strengthens the robustness of findings by revealing co-movement phases and localized synchronization between variables and strengthening the robustness of the findings. XWT provides additional insights into the synchronization between cyberattack events and market volatility, validating patterns identified through TVP-VAR and CWT. This dual time-frequency approach, when integrated with rolling window estimation, provides a comprehensive framework capable of capturing both the temporal evolution and spectral distribution of cyber-financial interlinkages.

Together, the TVP-VAR, CWT, and XWT methods form a multi-dimensional analytical structure that effectively captures the complex, nonlinear, and time-dependent nature of cyber risk transmission in clean energy financial markets.

3.3.1. TVP-VAR Model Framework

The TVP-VAR model is implemented to estimate dynamic interdependencies between cyberattacks and CE market indices. By allowing coefficients to vary over time, the model tracks shifts in market sensitivity and propagates the effects of cyber shocks across multiple financial channels.

The methodology of Koop and Korobilis [44] was employed to estimate the dynamic interactions between cyberattacks and CE indices. The model enables the propagation of cyber shocks over time and the detection of structural changes in market sensitivity. Its applicability has been demonstrated in several studies on financial volatility driven by geopolitical and economic risks [49]. In this research, the TVP-VAR framework is adapted using the specification introduced by Gabauer and Gupta [45] to capture time-varying interdependencies among variables.

$$X_t = \beta_t X_{t-1} + p_t,\ p_t \sim G(0, S_t), \tag{3}$$

$$\beta_t = \beta_{t-1} + q_t,\ q_t \sim G(0, R_t). \tag{4}$$

Here, X_t and X_{t-1} are the vectors of current and lagged variables. B_t is a time-varying coefficient matrix, while S_t and R_t are the variance–covariance matrices of the error terms. The model also calculates bidirectional and net connectivity indices between variables using the decomposition of forecast errors (GFEVD) [50]. The variance of step error h in forecast variable i is due to shocks to variable j.

$$\widetilde{\phi}^{g}_{ij,t}(m) = \frac{\sum_{t=1}^{m-1} \psi^{2,g}_{ij,t}}{\sum_{j=1}^{G} \sum_{t=1}^{m-1} \psi^{2,g}_{ij,t}} \tag{5}$$

Here, $\widetilde{\phi}^{g}_{ij,t}(m)$ denotes the m-step ahead GFEVD, $\sum_{j=1}^{G} \widetilde{\phi}^{g}_{ij,t}(m) = 1$, and $\sum_{ij=1}^{G} \widetilde{\phi}^{G}_{ij,t}(m) = G$. The definition of the total directional spillover TO other from variable i to all variables j in the TVP-VAR framework is as follows.

$$TO_{jt} = \zeta^{g}_{i \to j,t}(m) = \frac{\sum_{j=1,\, i \neq j}^{G} \widetilde{\phi}^{g}_{ij,t}(m)}{\sum_{j=1}^{G} \widetilde{\phi}^{g}_{ij,t}(m)} \cdot 100 \tag{6}$$

The relationship below expresses the total directional influence FROM others, measuring the spillover that variable i receives from other variables j:

$$FROM_{jt} = \zeta^{g}_{i\leftarrow j,t}(m) = \frac{\sum_{j=1,\, i\neq j}^{G} \tilde{\phi}^{g}_{ij,t}(m)}{\sum_{j=1}^{G} \tilde{\phi}^{g}_{ij,t}(m)} \cdot 100 \quad (7)$$

The difference between TO and FROM is the total net directional connection, as follows:

$$NET_{jt} = TO_{jt} - FROM_{jt} = \zeta^{g}_{i\rightarrow j,t}(m) - \zeta^{g}_{i\leftarrow j,t}(m)_{jt} \quad (8)$$

A positive result indicates a net transmitter, while a negative result indicates a net receiver. Global connection (GC) is determined as follows:

$$GC_{ij} = \frac{\sum_{j=1}^{G} TO_{jt}}{G} = \frac{\sum_{j=1}^{G} FROM_{jt}}{G}. \quad (9)$$

3.3.2. CWT Method

This study employed CWT to analyze the timing and frequencies of cyberattacks concerning stock market indices. CWT decomposes a time series into both time and frequency dimensions, providing a localized view of how relationships between variables evolve. This is particularly valuable in capturing the non-stationary, multi-scale nature of cyber risk impacts in financial markets. The CWT is mathematically expressed as

$$W_{\gamma}(u,v) = \int_{-\infty}^{\infty} \gamma(t)\Psi^{*}_{u,v}(t)dt, \quad (10)$$

where $\gamma(t)$ is the time series. $\Psi_{u,v}$ is the scaled and translated wavelet function, defined by the parameters u, the scale, which determines the level of detail (inversely proportional to frequency). Finally, v is the position in time, and $\Psi^{*}_{u,v}$ is the wavelet function's complex conjugate.

Morlet wavelet is used as the mother wavelet due to its balance between time and frequency localization, defined as

$$\Psi^{M}(t) = \pi^{-\frac{1}{4}} \cdot e^{i\omega_0 t} \cdot e^{-\frac{t^2}{2}}, \quad (11)$$

where ω_0 represents the center of the wavelet's frequency, and i is this intricate and analytical wavelet's imaginary component, having as a center point $(0, \omega_0/2\pi)$ inside the time-frequency range.

The wavelet power spectrum (WPS) is used to evaluate the intensity of variations, defined as

$$WPS_{u(v)} = \left|W_{\gamma}(u,v)\right|^2. \quad (12)$$

This approach generates a heatmap to indicate the amplitude of local variations as a function of time and frequency.

Wavelet coherence permits the examination of the connections between two time series, $\gamma(t)$ and $\delta(t)$, as

$$R^2_{\gamma,\delta}(u,v) = \frac{\left|S\left(W_{\gamma}(u,v) * W^{*}_{\delta}(u,v)\right)\right|^2}{S\left(\left|W_{\gamma}(u,v)\right|^2\right) \cdot S(|W_{\delta}(u,v)|^2)}, \quad (13)$$

where $W_{\gamma}(u,v)$ and $W_{\delta}(u,v)$ are the wavelet transforms of the series $\gamma(t)$ and $\delta(t)$. $S(\cdot)$ is the smoothing function, and $R^2(u,v)$ indicates the level of correlation between the two series according to time and frequency (0 = no relationship; 1 = maximum relationship).

To enhance temporal resolution, the CWT analysis is integrated with a rolling window approach. The sample period (2018–2025) is segmented into nine overlapping windows

of 320 days each. This segmentation enables the detection of regime shifts, synchronization bursts, or temporary breakdowns in market response to cyber risk.

3.4. Robustness Tests

The XWT method was applied to validate the robustness of the outcomes. This approach combines the strengths of the CWT and WTC, enabling a comprehensive analysis of the relationships between time series. XWT provides insights into the amplitude of coherence and phase relationships, offering a deeper understanding of the interplay between variables. Through XWT, the wavelet transforms of two time series are combined to generate the cross-wavelet spectrum, mathematically expressed as

$$W_{\gamma\delta}(u,v) = W_{\gamma}(u,v) \cdot W_{\delta}^{*}(u,v). \quad (14)$$

Spectrum magnitude $\left(\left|W_{\gamma\delta}(u,v)\right|\right)$ indicates the combined power of the signals at a given scale and temporal position, while the spectrum phase ($\arg(W_{\gamma\delta}(u,v))$) indicates the phase relationship between the series. The XWT spectrum is plotted with time on the horizontal axis and scale (inversely proportional to frequency) on the vertical axis. This approach provides a detailed visualization of the dynamic relationships between two time series.

4. Results

This section uses an integrated methodological framework to analyze the connection between cyberattacks and financial market volatility in the CE sector. By combining advanced time-series analysis techniques, our study offers a nuanced understanding of how digital risks influence financial markets.

4.1. Statistical Summary

Analyzing the descriptive statistics for CE indices from 2018 to 2025 highlights high volatility and asymmetric return distributions (Table 2). The most volatile indices—TAN (4.42) and PBW (4.50)—suggest increased sensitivity to major cyber events and external factors. At the same time, the relative stability of the RNRG index (1.54) indicates lower exposure to these risks. High kurtosis values reflect the frequency of extreme events, while positive skewness indicates the tendency of markets to recover quickly following shocks.

The Jarque–Bera test outcomes show that all indices' return distributions significantly deviate from normality ($p < 0.01$), underlining the nonlinear and complex nature of financial dynamics in CE markets. The negative skewness across all indices indicates a higher probability of extreme losses than gains, while the elevated kurtosis values suggest fat tails. These features reinforce the importance of capturing the effects of unexpected shocks, such as cyberattacks, on market behavior. The interquartile range (IQR) illustrates the dispersion within the central 50% of returns. Higher IQR values, such as PBW (3.26), imply more pronounced variability and volatility, whereas lower IQRs, like RNRG (1.40), denote relatively stable return patterns.

Table 2. Statistical summary.

Index	Mean	Median	Max.	Min.	Std. Dev.	Skew.	Kurt.	Prob.	IQR
ICLN	0.022	0.000	10.80	−13.71	1.918	−0.406	9.130	0.000	2.00
TAN	0.037	−0.006	12.66	−17.54	2.670	−0.204	6.493	0.000	3.03
QCLN	0.031	0.105	13.64	−13.91	2.461	−0.168	5.602	0.000	2.84
CNRG	0.039	0.029	11.63	−14.14	2.228	−0.215	6.530	0.000	2.51
ACES	−0.002	0.037	11.82	−14.38	2.309	−0.224	6.287	0.000	2.55
PBW	−0.017	0.000	13.50	−15.64	2.742	−0.161	5.215	0.000	3.26

RNRG	−0.017	0.000	8.784	−10.38	1.383	−0.597	10.46	0.000	1.40
ACWI	0.035	0.075	7.821	−11.90	1.196	−1.049	17.41	0.000	1.55
IEUR	0.022	0.088	8.714	−12.39	1.289	−1.251	17.81	0.000	1.26
EEMA	0.015	0.032	8.401	−12.35	1.387	−0.601	11.58	0.000	1.56
EWZ	−0.027	0.070	16.23	−26.26	2.340	−1.436	20.56	0.000	2.34
EZA	0.003	0.040	9.613	−16.04	2.010	−0.740	10.45	0.000	2.21
AFK	−0.010	0.050	8.460	−12.33	1.437	−1.119	13.37	0.000	1.51

Note: This table provides descriptive statistics for CE indexes and ETFs, including measures of central tendency, dispersion, and distribution.

4.2. Stationarity Tests

The results of the stationarity tests applied to the CE indices confirm that all-time series are stationary, either at level or in first difference, and are thus suitable for econometric analysis. The Augmented Dickey–Fuller (ADF) and Phillips–Perron (PP) tests yielded test statistics that are significantly more negative than the corresponding critical values, with associated *p*-values equal to 0.000, allowing for the rejection of the null hypothesis of a unit root (Table 3). Additionally, the Kwiatkowski–Phillips–Schmidt–Shin (KPSS) test produced LM statistics below the critical thresholds at all conventional significance levels, supporting the null hypothesis of stationarity.

Table 3. Stationarity tests.

Index	ADF t-Stat. Level	Prob. *	t-Stat. 1st Diff	Prob. *	PP Adj. T-Stat Level	Prob. *	Adj. T-Stat 1st Diff	Prob. *	KPSS LM-Stat. Level	Prob. *	LM-Stat. 1st Diff	Prob. *
ICLN	−25.90	0.000	−19.76	0.000	−40.26	0.000	−490.2	0.000	0.294	0.640	0.003	0.979
TAN	−40.38	0.000	−20.74	0.000	−40.38	0.000	−369.2	0.000	0.637	0.578	0.002	0.990
QCLN	−40.43	0.000	−20.31	0.000	−40.43	0.000	−433.5	0.000	0.471	0.614	0.001	0.990
CNRG	−26.83	0.000	−20.11	0.000	−41.38	0.000	−416.0	0.000	0.479	0.483	0.001	0.987
ACES	−40.20	0.000	−19.93	0.000	−40.22	0.000	−457.0	0.000	0.523	0.973	0.003	0.984
PBW	−39.99	0.000	−20.17	0.000	−39.99	0.000	−394.1	0.000	0.606	0.807	0.002	0.985
RNRG	−26.37	0.000	−18.88	0.000	−41.02	0.000	−631.4	0.000	0.293	0.619	0.014	0.997
ACWI	−12.32	0.000	−20.75	0.000	−45.54	0.000	−549.8	0.000	0.043	0.248	0.017	0.971
IEUR	−14.50	0.000	−18.85	0.000	−43.35	0.000	−628.7	0.000	0.036	0.494	0.015	0.979
EEMA	−46.27	0.000	−21.64	0.000	−46.07	0.000	−644.2	0.000	0.092	0.668	0.005	0.971
EWZ	−27.95	0.000	−21.45	0.000	−46.82	0.000	−739.8	0.000	0.023	0.640	0.006	0.957
EZA	−43.36	0.000	−22.00	0.000	−43.30	0.000	−930.9	0.000	0.031	0.947	0.001	0.971
AFK	−16.31	0.000	−22.34	0.000	−43.71	0.000	−1259.9	1.000	0.057	0.779	0.015	0.964

Note: Table shows the outcomes of the stationarity tests employed on the variables included in the study using the ADF, PP, and KPSS tests. The asterisk (*) indicates statistical significance at the 1% level.

4.3. Main Results of Econometric Analyses

4.3.1. TVP-VAR Model Results

The TVP-VAR analysis reveals a time-varying and statistically meaningful relationship between cyberattacks and volatility spillovers in CE stock indices. Notably, TAN and ICLN exhibited pronounced short-term sensitivity to cyber risk events. TAN reached a maximum spillover effect of 12.4% in Q1 2021, while ICLN recorded a comparable peak of 11.8% in Q2 2021. These spikes underline the heightened vulnerability of the solar energy sector, potentially driven by its complex and highly digitized infrastructure. In

contrast, indices such as RNRG and PBW, which represent more diversified portfolios across geographies and technologies, displayed lower average spillover values, ranging between 5.2% and 6.4%. This contrast supports the hypothesis that diversification acts as a buffer against concentrated cyber threats, attenuating the overall transmission of risk to specific market segments (Appendix A).

Elevated dynamic coherence between cyber risk indicators and CE indices was observed mainly over short-term horizons (1–3 months), with a notable peak of 0.77 in Q2 2020. This pattern reflects a surge in volatility immediately following cyber incidents, followed by a rapid decline in coherence levels. Such behavior underscores the CE sector's capacity to absorb shocks and adapt to cyber-related disruptions over time, highlighting its increasing resilience in the face of digital threats.

The severity of cyberattacks exerts a significant influence on CE stock indices, with the strongest effects observed in more specialized ETFs such as ICLN, TAN, and QCLN. The link between attack severity and market volatility becomes especially pronounced during periods of elevated uncertainty, suggesting that higher severity scores intensify perceived risk, prompting swift investor reactions. TAN experienced the largest volatility increase associated with attack severity, reaching 14.1% in Q1 2021, followed closely by ICLN at 13.6%. In contrast, broader and more diversified indices such as PBW and RNRG registered only moderate increases of 6.8% and 5.9%, respectively. This inverse relationship between portfolio diversification and sensitivity to attack severity highlights the crucial role of diversification in mitigating cyber-related financial risks.

During global crises such as the Ukraine conflict, cyberattack severity scores intensified market volatility, with coherence levels peaking at 0.79 for sector-focused CE indices and 0.62 for more diversified portfolios. This finding highlights the complex interaction between macroeconomic uncertainty and cyber threats, where concentrated indices exhibit sharper and more immediate responses to digital shocks.

TVP-VAR results confirm that cyberattacks targeting critical infrastructure can lead to substantial disruptions in CE markets. TAN, ICLN, and QCLN experienced notable short-term volatility following such events. For instance, TAN recorded a 13.2% volatility spike in the aftermath of the Q2 2020 attacks, while ICLN saw an increase of 12.4%. These sharp reactions suggest that investors reassess risk more drastically when operational vulnerabilities are exposed in concentrated sectors.

Diversified indices such as PBW and RNRG responded with more moderate volatility increases of 6.1% and 5.3%, respectively. This divergence underscores the importance of diversification strategies in preserving financial stability, even when cyberattacks compromise critical infrastructure components.

The short-term impact of targeted cyberattacks was most pronounced immediately following the incident, with markets exhibiting peak volatility responses in the immediate aftermath. However, elevated volatility persisted in more vulnerable segments, such as the solar energy sector, where fluctuations remained above baseline levels for up to two months.

Moreover, these targeted attacks tended to intensify during periods of economic instability or broader market turbulence, further amplifying investor risk perceptions. This dynamic was particularly evident in Q3 2020, when coherence values reached 0.75, underscoring the heightened sensitivity of CE markets to overlapping systemic shocks.

4.3.2. CWT Results

The CWT analysis, conducted using a rolling window framework, revealed significant temporal variations in the relationship between cyberattack frequency and financial market volatility across seven overlapping time segments (see Appendix B). Results indicate that cyberattack frequency is a key short-term driver of volatility, with TAN and

ICLN showing the strongest responses. These indices recorded peak wavelet coherence values of 0.82 and 0.78, respectively, during the critical period spanning Q2 2020 to Q1 2021. This interval coincides with the COVID-19 pandemic, a time marked by accelerated digitalization and elevated systemic cyber risks, which exacerbated investor uncertainty. Notably, the most intense volatility responses occurred within one to three months following cyber events, highlighting the market's high responsiveness to cyber shocks.

More diversified indices such as PBW and RNRG demonstrated comparatively higher stability, with lower wavelet coherence values of 0.55 and 0.50, respectively, during the same period. Their broader geographical and sectoral allocation appears to mitigate concentrated exposure to cyber-related risks. This result aligns with the findings of Dogan et al. [51], who emphasized that diversification remains a fundamental strategy for managing systemic shocks, including those induced by cyberattacks.

The severity of cyberattacks, quantified using the OWASP methodology, further emphasized the differential impact across CE indices. High-severity incidents—characterized by severity scores exceeding 4.0—had a pronounced effect on TAN and ICLN, with wavelet coherence values peaking at 0.85 and 0.80, respectively, during Q1 2021. While generally more stable, PBW still exhibited noticeable fluctuations in response to major cyber events, indicating the vulnerability of some of its underlying components. In contrast, RNRG maintained a relatively stable profile, with coherence values remaining around 0.6 even during high-severity periods, reaffirming the stabilizing influence of diversified exposure.

Indices such as CNRG and ACES, which represent companies with strong dependencies on advanced digital technologies and energy storage systems, exhibited pronounced volatility during periods marked by intensified cyberattacks. For example, CNRG reached wavelet coherence levels of up to 0.70 in Q3 2020, underscoring the vulnerability of innovation-driven CE firms to disruptions affecting critical digital infrastructure. Similarly, ACES showed significant sensitivity to cyberattacks targeting energy storage and distribution systems, with coherence peaking at 0.72 in Q4 2020. These results are consistent with the findings of Vargas and Tien [52], who emphasize the heightened susceptibility of interconnected infrastructures, particularly in light of emerging technologies such as 5G, which expand the digital attack surface.

Over the long term, the relationship between cyberattacks and financial market volatility became less pronounced. Indices such as RNRG and ACES gradually absorbed the shocks associated with cyber incidents, contributing to broader market stabilization. This adaptive behavior is reflected in declining wavelet coherence values—dropping below 0.4 after Q2 2021—which suggests an increasing ability within the CE sector to mitigate cyber-related disruptions through enhanced cybersecurity investments and organizational resilience. These findings are in line with Pettersen and Grøtan [53], who highlight the importance of strategic risk management in reducing the long-term vulnerabilities of interconnected digital infrastructures.

The contrasting patterns observed between concentrated indices (such as TAN and ICLN) and diversified ones (such as PBW and RNRG) reinforce the critical role of portfolio diversification as an effective risk mitigation strategy. Furthermore, the findings point to the urgent need for targeted cybersecurity interventions, particularly in high-risk areas such as energy storage and distribution infrastructure. These insights provide valuable guidance for investors and policymakers aiming to enhance the resilience of CE markets in the face of increasingly sophisticated and frequent cyber threats.

4.3.3. Robustness Results

The XWT analysis was conducted across nine overlapping time windows to assess the robustness and consistency of the findings derived from the TVP-VAR and CWT models. The results corroborate the wavelet coherence analysis, revealing strong short-term synchronization between cyberattack frequency and financial market volatility (Appendix C). Notably, TAN and ICLN exhibited elevated coherence values of 0.84 and 0.79, respectively, during the period from Q2 2020 to Q1 2021, highlighting heightened market sensitivity amidst the macroeconomic uncertainty brought about by the COVID-19 pandemic. PBW and RNRG displayed lower coherence levels—0.58 and 0.54—reinforcing the stabilizing role of diversified portfolio structures in mitigating cyber risk-induced volatility.

The XWT results highlight significant differences between indices based on their portfolio composition. TAN and ICLN experienced more pronounced volatility during high-severity cyberattacks, with amplitude peaks corresponding to periods when OWASP severity scores exceeded 4.0. In contrast, diversified indices like PBW and RNRG exhibited reduced synchronization with cyberattack frequency, reflecting greater resilience to external digital shocks. This contrast was particularly evident in Q1 2021, when OWASP severity scores peaked at 3.5. During this period, PBW maintained relatively low amplitude responses, underscoring its stability compared to the heightened fluctuations observed in TAN.

The XWT analysis offers compelling evidence of short-term market sensitivity and long-term resilience in response to cyberattacks, reinforcing the critical role of portfolio diversification and proactive risk management strategies. These insights are particularly relevant for mitigating the financial repercussions of cyber threats within the CE sector.

5. Discussion

This study's findings highlight the significant impact of cyberattacks on financial market volatility in the CE sector, particularly in the short term. The results indicate that financial markets are highly sensitive to the frequency and intensity of cyberattacks, reinforcing the argument that cyber resilience can serve as a competitive advantage for companies operating in the CE industry. Sallos et al. [54] emphasize that aligning operational strategies with robust cybersecurity risk management practices is critical to mitigating these adverse effects and enhancing market stability.

Our findings reveal that cyberattacks act as shock transmitters to CE ETFs, consistent with the results of Ziadat et al. [55], who identified the Global Clean Energy Index as a net receiver of market information, while the Renewable Energy and Clean Technology Index functions as a net sender. These findings reinforce the importance of understanding sectoral dependencies and investor sentiment in CE financial markets, particularly in the face of escalating digital threats.

Furthermore, our results align with those of Gabriel and Pinho [56], who found that CE assets demonstrate positive returns when facing climate-related uncertainty, in contrast to the negative impact experienced by fossil fuel sector assets and black energy markets. A similar pattern emerges under cybersecurity stress − diversified CE portfolios display lower volatility and faster recovery, suggesting that green energy assets may serve as a buffer against systemic risk.

5.1. Sectoral Sensitivities and the Role of Diversification in CE Markets

The wavelet coherence scalograms indicate that the CE sector exhibits substantial variability in market responses to cyberattacks. Indices such as TAN and ICLN display significant short-term fluctuations, reinforcing their heightened vulnerability to digital risks. This reflects the growing dependence of CE investments on digitalized infrastructure, including smart grids, blockchain-based energy trading, and IoT-enabled monitoring systems. The global CE investment reached 1.8 trillion US dollars in 2023, emphasizing the urgent need for enhanced cybersecurity standards in the sector [57]. The high exposure of solar and wind sectors to digital technologies intensifies their susceptibility to cyber threats, exacerbating investor risk perceptions. These findings align with Yao et al. [58], who demonstrated the multifractal nature of CE stock markets and their asymmetric correlations with crude oil markets, particularly during periods of financial stress. This multifractal behavior helps explain the rapid volatility shifts observed in more concentrated CE indices following cyber events.

In contrast, diversified indices such as PBW and RNRG exhibit greater stability, benefiting from broader geographical and technological diversification. These indices reduce dependency on specific vulnerable market segments, acting as a buffer against localized cyber shocks. Arcuri et al. [59] emphasized that diversification is a crucial risk mitigation strategy, particularly for industries with complex supply chains, such as solar energy. The TAN index, which primarily consists of solar energy firms, is particularly susceptible to cyberattacks targeting energy storage technologies and smart distribution systems.

The resilience of diversified indices such as PBW and RNRG reinforces the argument that portfolio diversification reduces systemic vulnerabilities. These indices balance exposure across multiple energy segments and geographic regions, reducing the concentration risk associated with sector-specific cyber threats. Dogan et al. [51] also highlighted that asymmetry in volatility and returns between CE assets and broader stock markets reinforce the importance of diversification in mitigating external financial shocks.

Moreover, technological advancements play a pivotal role in shaping sectoral exposure to cyber risks. Vargas and Tien [52] examined the implications of 5G technology on cyber-physical vulnerabilities in interconnected infrastructure systems, emphasizing that increased reliance on emerging technologies significantly broadens the attack surface for CE companies. This is consistent with our findings for indices such as ACES and CNRG, which exhibited strong wavelet coherence with cyber risk variables during periods marked by technological disruption and infrastructure-targeted attacks. These insights suggest that as CE markets become increasingly integrated into digital ecosystems, their exposure to cyber threats will continue to grow, necessitating continuous enhancements in both risk management strategies and cybersecurity infrastructure.

5.2. Influence of the Severity and Targeting of Attacks on CE Markets

The severity and targeting of cyberattacks play a critical role in shaping financial market responses, particularly in terms of volatility and investor sentiment. Our wavelet-based findings confirm that high-severity cyberattacks disproportionately affect indices focused on emerging CE technologies, such as TAN and QCLN. These indices exhibited pronounced short-term volatility spikes and strong synchronization with cyber risk variables, especially during periods with OWASP severity scores exceeding 4.0 and attacks targeting critical digital infrastructures [30]. This heightened sensitivity is closely linked to their reliance on interconnected infrastructures such as smart grids, blockchain platforms, and IoT monitoring systems. The market's amplified risk perception becomes even more evident during episodes of macroeconomic stress, such as the COVID-19 pandemic or geopolitical crises like the war in Ukraine, which further intensify volatility in CE financial indices.

The interaction between digital and economic risks suggests that policymakers should adopt a dual approach, simultaneously addressing cyber resilience and macroeconomic stability. Investing in robust cybersecurity frameworks and resilient digital infrastructures is essential to mitigate the amplified risks that emerge during economic downturns. Additionally, integrating cyber risk considerations into macroeconomic policy planning could enhance market stability, particularly in digital-intensive sectors such as CE. These findings align with Xiao et al. [60], who demonstrated that energy transitions contribute to financial volatility, especially during periods of economic turbulence. In contrast, diversified indices such as RNRG and PBW exhibit greater resilience, underscoring the stabilizing effect of sectoral and geographical diversification in managing cyber-induced financial uncertainty.

From an investor behavior perspective, Wang and Wang [5] emphasized that unusual market reactions often emerge during periods of abnormal volatility, driven by differences in investor experience, information asymmetry, and varying risk attitudes. These behavioral dynamics are reflected in our findings, where CE indices—particularly concentrated ones like TAN and ICLN—exhibited amplified volatility following high-severity cyberattacks. The sharp co-movements and elevated amplitude observed in the wavelet domain suggest that investor panic may play a central role in accelerating short-term market fluctuations. These patterns highlight the need for behavioral-aware strategies in risk management and investor communication to reduce overreactions and promote stable market behavior.

A comprehensive cybersecurity risk management approach could help offset financial instability associated with cyberattacks, particularly in the CE sector, where technological reliance increases exposure to digital threats. Lee [61] emphasized that the adoption of structured cybersecurity policies is essential for reducing financial instability, particularly in industries that depend on digital infrastructure for energy production, trading, and distribution. These findings align with our study, showing that targeted cyberattacks on critical CE infrastructure amplify volatility in indices such as TAN and ICLN, given their dependence on complex and interconnected digital systems [10].

The economic consequences of high-severity cyberattack extend beyond immediate market fluctuations, generating direct financial losses, reputational harm, and sustained market uncertainty. These impacts are particularly evident in CE markets, where investor sentiment is highly sensitive to technological vulnerabilities. Our empirical findings confirm that indices like TAN and ICLN are especially exposed to such risks, whereas diversified indices such as PBW and RNRG exhibit greater resilience. Halgamuge [62] emphasized the potential of deep learning-based cybersecurity solutions in detecting and mitigating cyber threats, particularly for critical infrastructures in energy systems. Integrating AI-driven security models into the risk management strategies of CE firms could further enhance the robustness of diversified portfolios, offering long-term protection against cyber-induced financial shocks.

5.3. Interaction with the Macroeconomic Context

Cyberattacks play a significant role in amplifying financial market volatility, particularly during periods of macroeconomic instability. These events heighten investor risk perceptions, exacerbate financial market responses, and intensify economic shocks [14]. Wu and Liu [63] demonstrated that investor sentiment and climate policy uncertainty drive spillovers in green finance markets, especially during global crises. Their findings align with the strong correlations identified in this study between cyberattacks and financial volatility in CE markets during macroeconomic downturns. The interaction between cyber risks and economic instability triggers contagion effects, which disproportionately impact financial markets, exacerbating systemic vulnerabilities.

The impact of macroeconomic fluctuations on cyber risks in CE markets is further emphasized by Sharma et al. [64], who explored the relationships between green economy investments, sustainability, bitcoin, and oil prices. Their study revealed that macroeconomic variables strongly influence CE market dynamics, particularly during heightened periods of volatility. Similarly, Eisenbach et al. [6] provided a detailed pre-mortem analysis of cyber risks in the US financial system, highlighting the systemic vulnerabilities that arise from cyberattacks on critical infrastructures. Our wavelet coherence results confirm that indices such as TAN and ICLN exhibit intensified volatility during macroeconomic crises, as firms included in these indices tend to be more dependent on global economic conditions and heavily integrated into digital infrastructures.

The interconnected nature of financial markets further exacerbates these risks. Yadav et al. [65] confirmed the significant coherence between green bonds, stock markets, and energy commodities during the COVID-19 pandemic, reinforcing the vulnerability of CE markets to global financial instability. Similarly, Thi Xuan and Thai Hung [66] explored the time-frequency effects of nonrenewable energy investments and globalization, demonstrating how macro trends influence CE market performance under financial and digital risk pressures. Their findings suggest that green investments play a critical role in stabilizing markets, yet these investments are increasingly exposed to cyber threats, introducing multi-layered volatility channels that challenge traditional risk mitigation models.

Despite these vulnerabilities, diversified indices such as PBW and RNRG exhibit greater resilience to the combined impact of macroeconomic and cyber risks. Their geographic and sectoral diversification acts as a buffer, mitigating localized financial shocks and reinforcing the importance of portfolio diversification in managing systemic risks. Zhang et al. [67] further highlighted that global economic conditions have a pronounced effect on the volatility of CE ETFs, emphasizing the interconnectedness between macroeconomic trends and financial performance in CE markets.

Beyond financial volatility, the broader macroeconomic context influences investor behavior and sectoral risk correlations. Abakah et al. [68] demonstrated that eco-friendly financial markets exhibit stronger correlations with other economic sectors during global crises, highlighting the need for integrated risk management approaches that consider both cyber and macroeconomic risks. Osman and El-Gendy [69] similarly revealed that advanced economies remain highly vulnerable to cyberattacks, particularly in global trade, reinforcing the necessity of strengthening cybersecurity policies within financial market regulations. Farrand [70] further underscored the economy-security nexus by examining vulnerabilities in semiconductor supply chains, illustrating how cyber risks create cascading effects on global market stability.

6. Conclusions

This study highlights the significant impact of cyberattacks on the CE sector, particularly in technologically interconnected markets and vulnerable segments like solar energy. Our results demonstrate that the TAN and ICLN indices exhibit heightened short-term volatility in response to cyber threats, reflecting increased investor sensitivity to cybersecurity risks in concentrated CE portfolios. In contrast, PBW and RNRG indices show greater stability, benefiting from broader geographical and sectoral diversification, which helps absorb cyber-induced shocks. These findings emphasize that portfolio diversification serves as a critical risk-mitigation strategy against cybersecurity-related financial disruptions.

From an investment perspective, these results underscore the importance of balancing high-growth, technology-driven CE assets with diversified holdings that include a mix of renewable energy technologies and geographically distributed investments. Portfolios heavily weighted toward solar energy firms remain highly exposed to cyber-related

volatility spikes, while diversified holdings act as buffers against such shocks, reinforcing the value of risk-spreading strategies.

For policymakers, these findings reinforce the necessity of proactive cybersecurity investments and robust regulatory frameworks to safeguard critical infrastructure. Strengthening real-time threat detection systems and fostering collaboration between public and private sectors can significantly enhance market resilience and reduce systemic risks in the CE sector. Additionally, policy interventions that incentivize cybersecurity adoption across CE firms can mitigate the adverse financial consequences of cyberattacks. The integration of cybersecurity into environmental and financial policy agendas is essential as the CE sector becomes increasingly digitized and globally interconnected.

To further explore these insights, a scenario simulation analysis could assess the varying responses of different investment portfolios to cyber risks. Comparing high-concentration CE portfolios, heavily weighted toward solar and wind energy, with diversified portfolios incorporating various renewable energy segments and geographic exposures would provide a deeper understanding of the trade-offs between growth potential and risk exposure. Future research could also extend this analysis by integrating macroeconomic conditions, regulatory policy changes, and investor sentiment dynamics to assess their moderating effects on cyber risk transmission in financial markets.

Additionally, while this study employs the OWASP methodology to quantify cyberattack severity, future research could explore alternative cybersecurity assessment frameworks, such as the NIST Common Vulnerability Scoring System and the MITRE ATT&CK methodology. These frameworks offer more detailed attack vector classifications and vulnerability assessments, potentially improving the precision of cyber risk quantification in financial modeling.

This study makes a distinct contribution to the emerging literature on the intersection between cyber risks and financial markets by integrating the frequency, severity, and targeting of cyberattacks into an advanced econometric framework. Utilizing TVP-VAR and wavelet-based techniques, this study captures the evolving nature of cyber risks across different market conditions. However, several limitations remain. A more granular modeling of exogenous forces—ranging from macroeconomic volatility and geopolitical instability to AI-powered security solutions—could deepen future insights into the transmission of cyber threats to CE financial performance.

Author Contributions: Conceptualization, C.G. and O.P.; methodology, C.G. and O.P.; software, C.G. and O.P.; validation, C.G. and O.P.; formal analysis, C.G. and O.P.; investigation, C.G. and O.P.; resources, C.G. and O.P.; data curation, C.G. and O.P.; writing—original draft preparation, C.G. and O.P., writing—review and editing, C.G. and O.P.; visualization, C.G. and O.P.; supervision, C.G. and O.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available on reasonable request from the corresponding author.

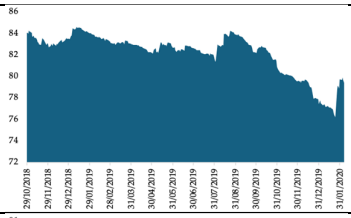
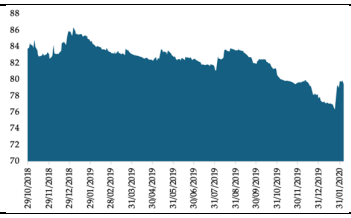
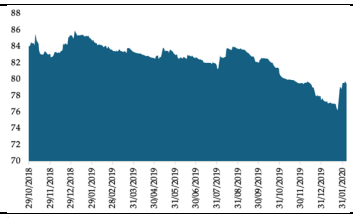
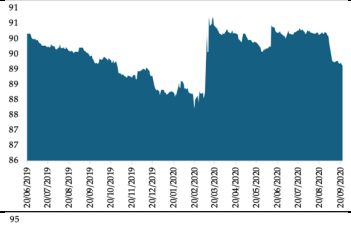
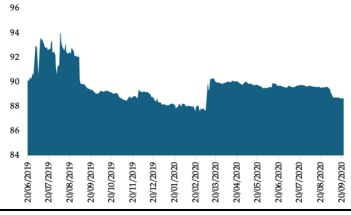
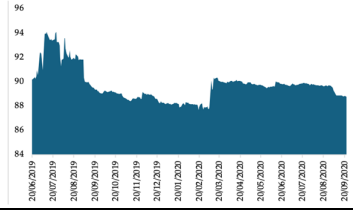
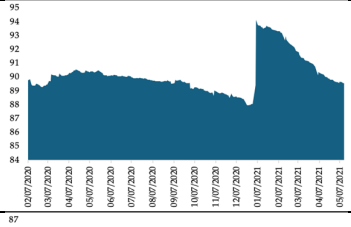
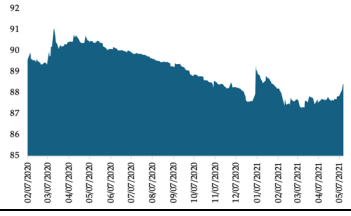
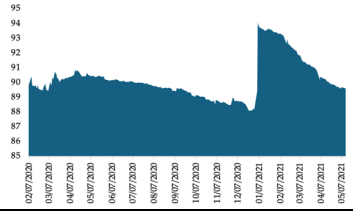
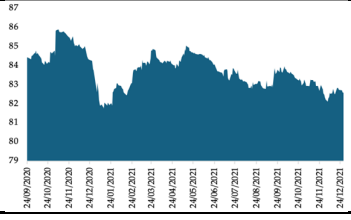
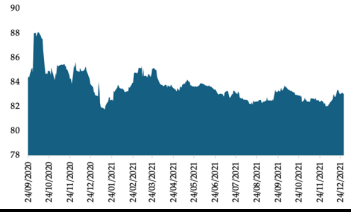
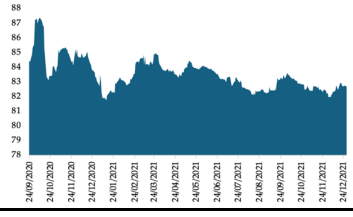
Conflicts of Interest: The authors declare no conflicts of interest.

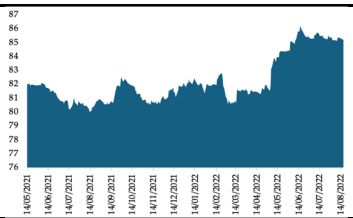
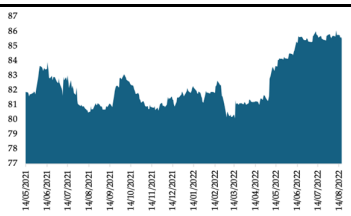
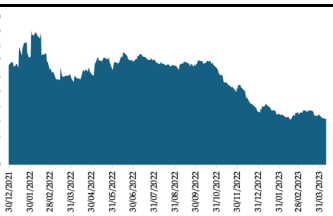
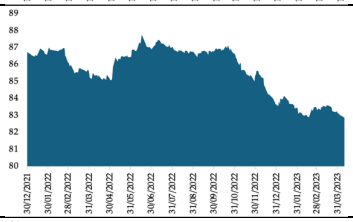
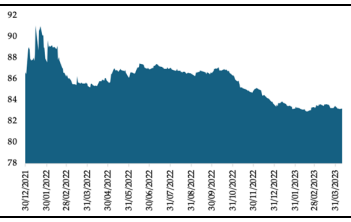
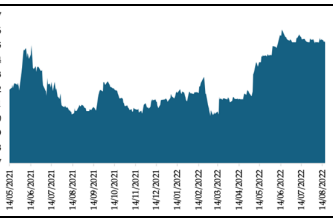
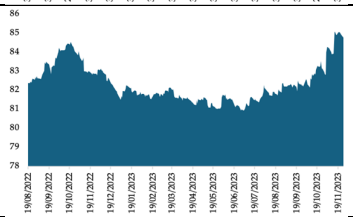
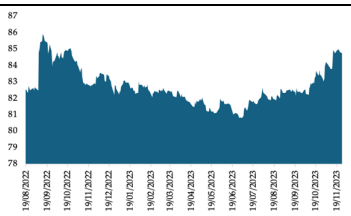
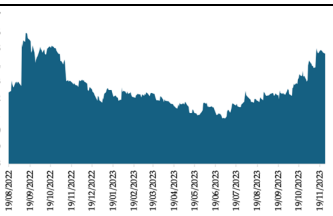
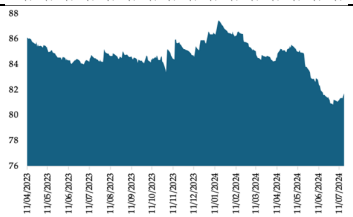
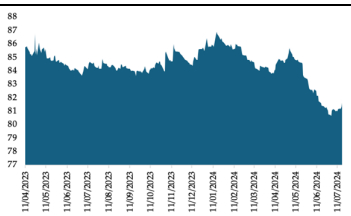
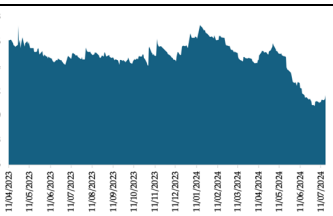
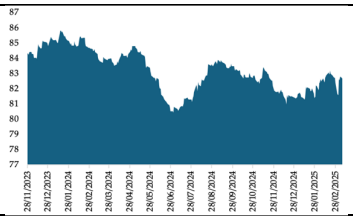
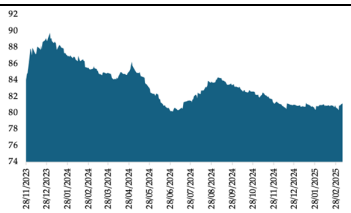
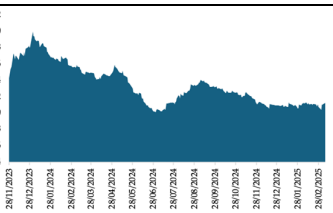
Abbreviations

The following abbreviations are used in this manuscript:

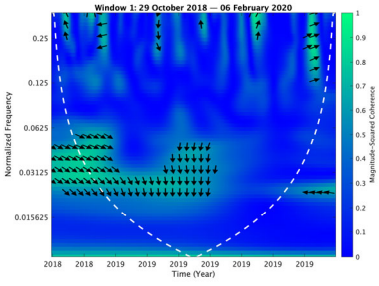
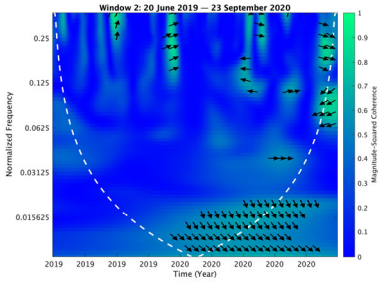
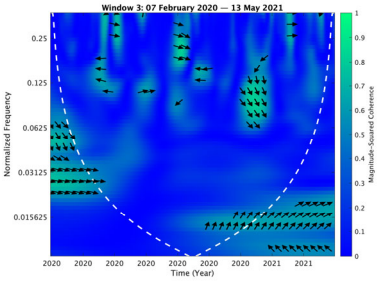
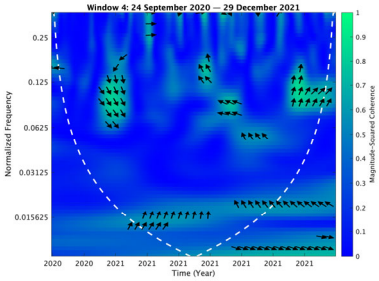
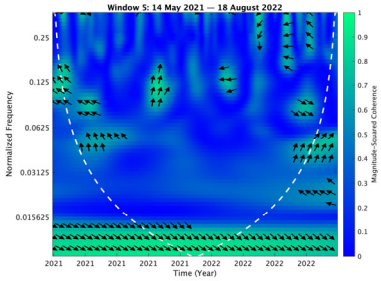
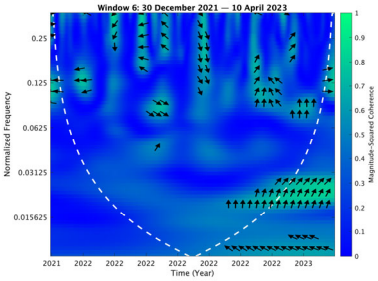
CE	Clean Energy
IoT	Internet of Things
ETFs	Exchange-Traded Funds
TVP-VAR	Time-Varying Parameter Vector Autoregression
OWASP	Open Web Application Security Project
AI	Artificial Intelligence
ICLN	iShares Global Clean Energy ETF
TAN	Invesco Solar ETF
QCLN	First Trust NASDAQasdaq Clean Edge Green Energy ETF
CNRG	SPDR Kensho Clean Power ETF
ACES	ALPS Clean Energy ETF
PBW	Invesco Wilder Hill Clean Energy ETF
RNRG	Global X Renewable Energy Producers ETF
CA	Number of Cyberattacks
SS	Severity Score
CI	Targeted Critical Infrastructure
CWT	Continuous Wavelet Transform
XWT	Cross-Wavelet Transform
GFEVD	Generalized Forecast Error Variance Decomposition
IQR	Interquartile Range
ADF	Augmented Dickey–Fuller
PP	Phillips–Perron
KPSS	Kwiatkowski–Phillips–Schmidt–Shin

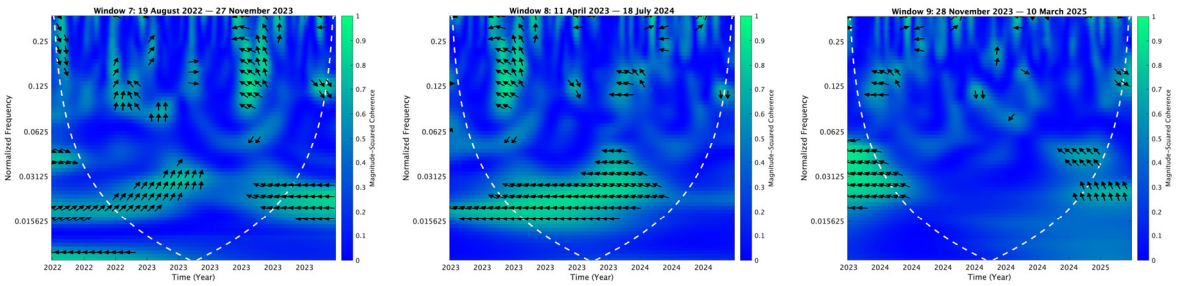
Appendix A. Results of TVP-VAR Analysis

Window	CA	SS	CI
1			
2			
3			
4			

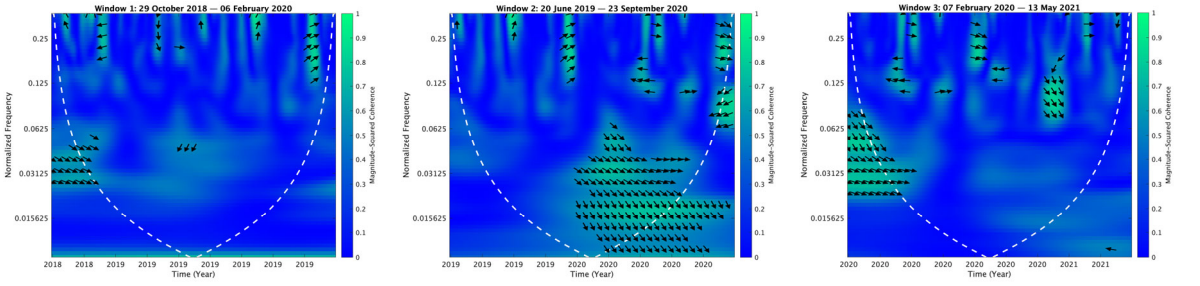
5			
6			
7			
8			
9			

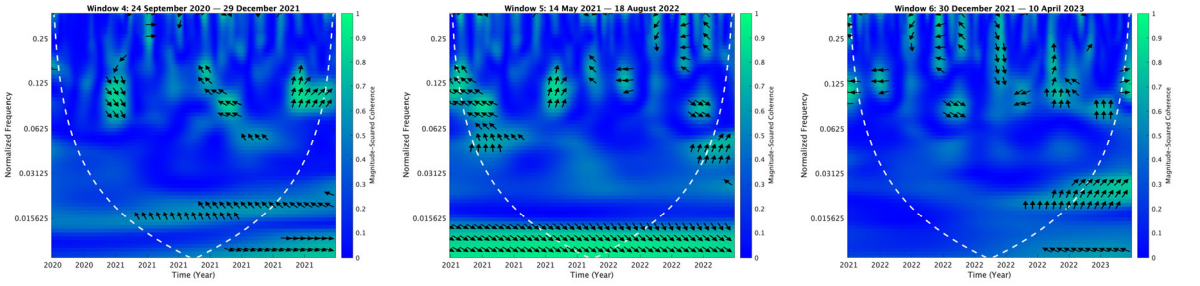
Appendix B. Wavelet Analysis Results

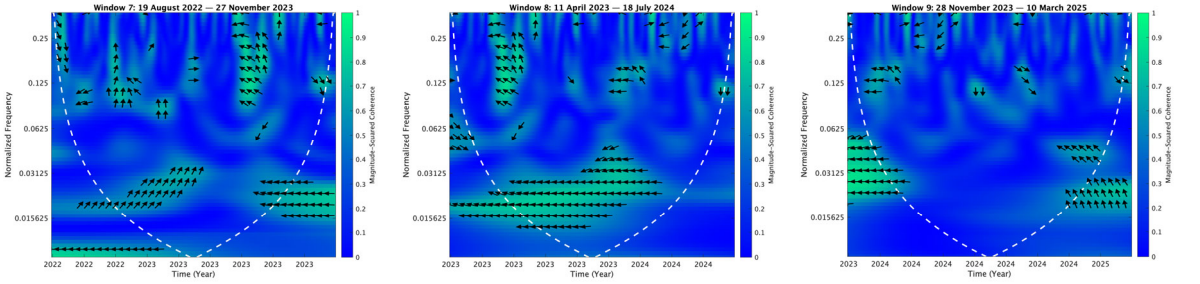
Index	CWT Windows		
ICLN			
			


Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

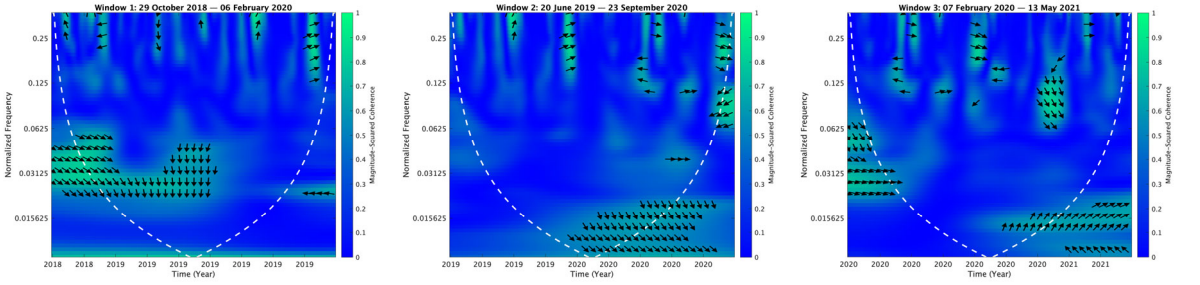
CA

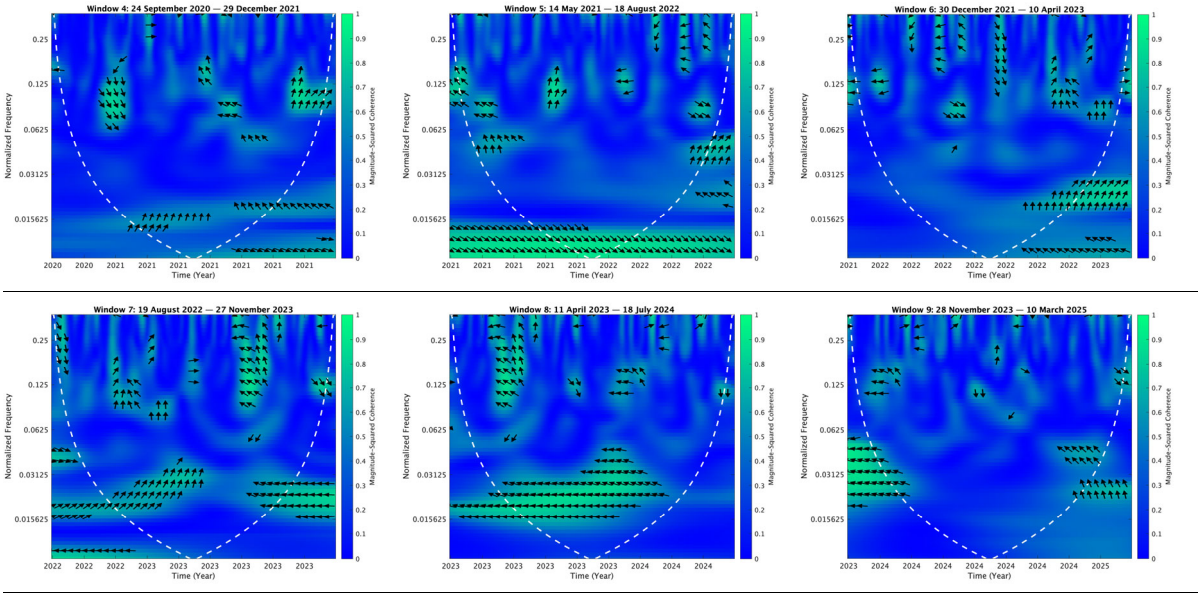

Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence


Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence


Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

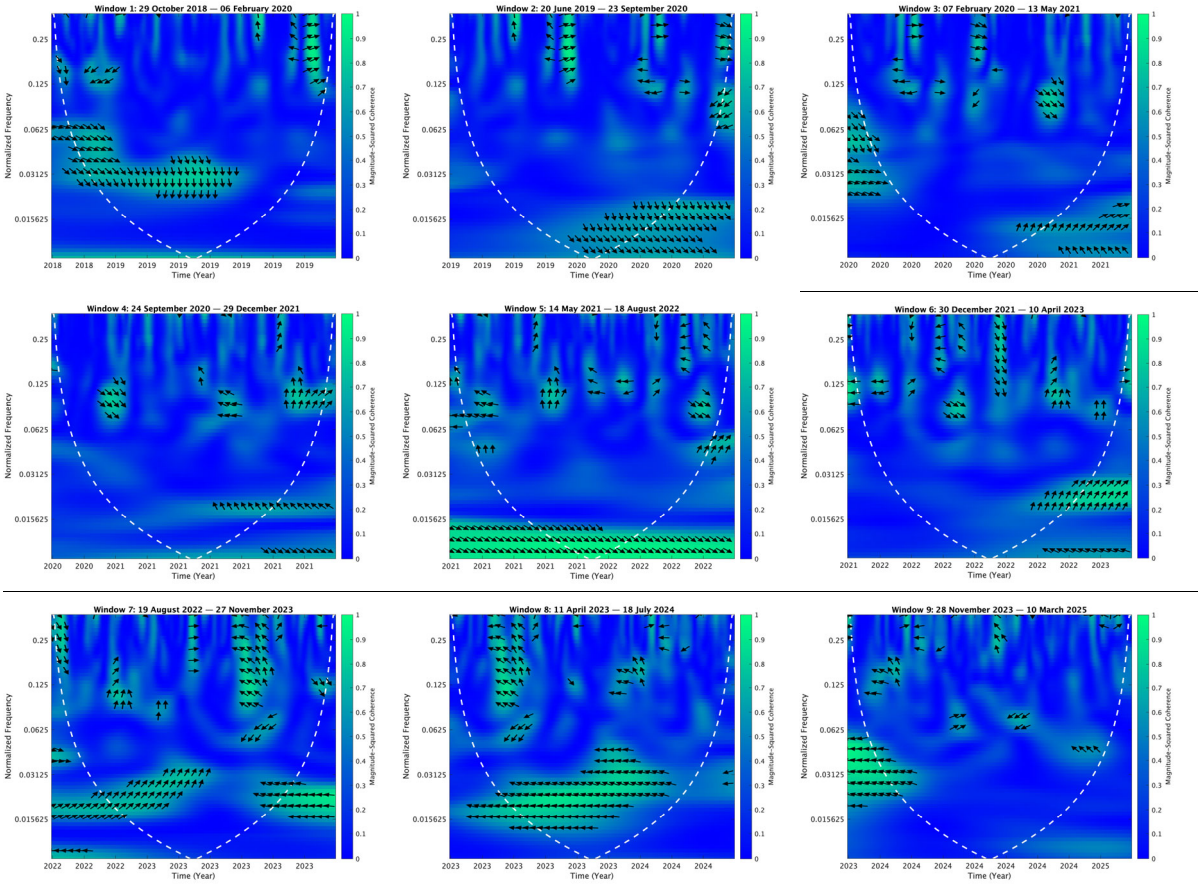
SS


Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

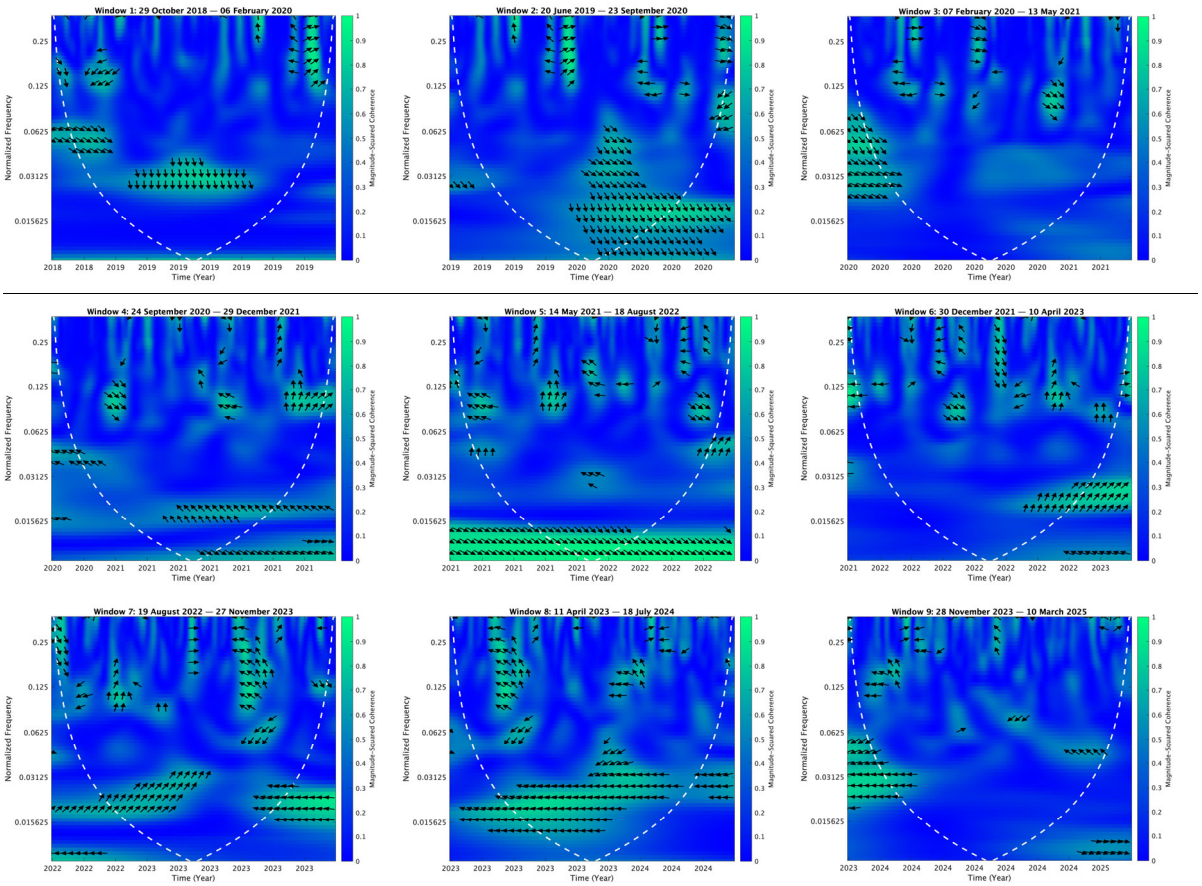

Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

CI

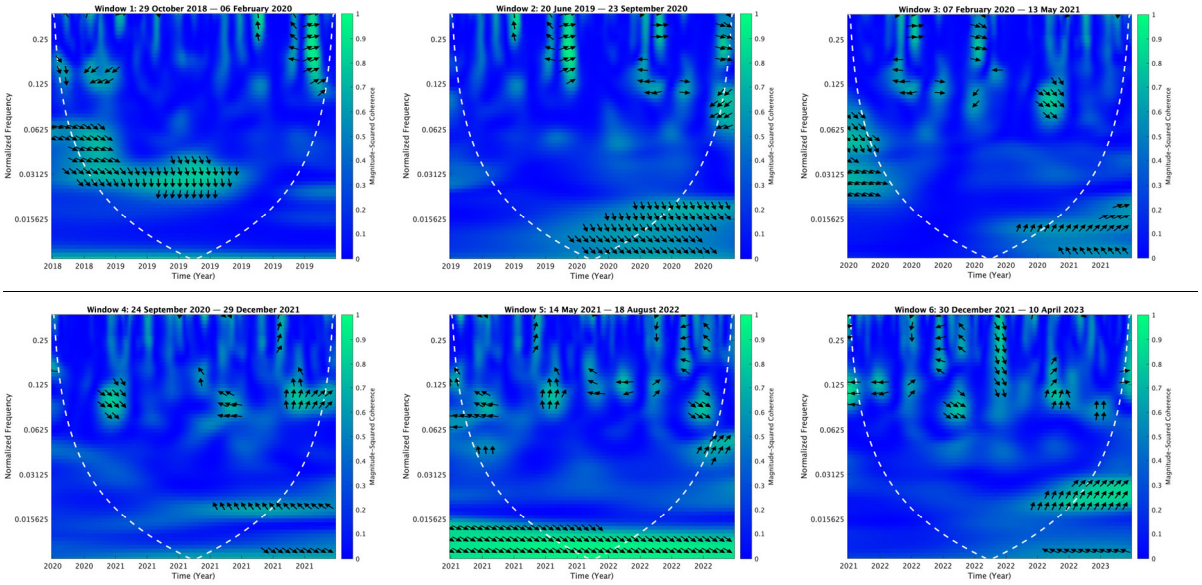
TAN

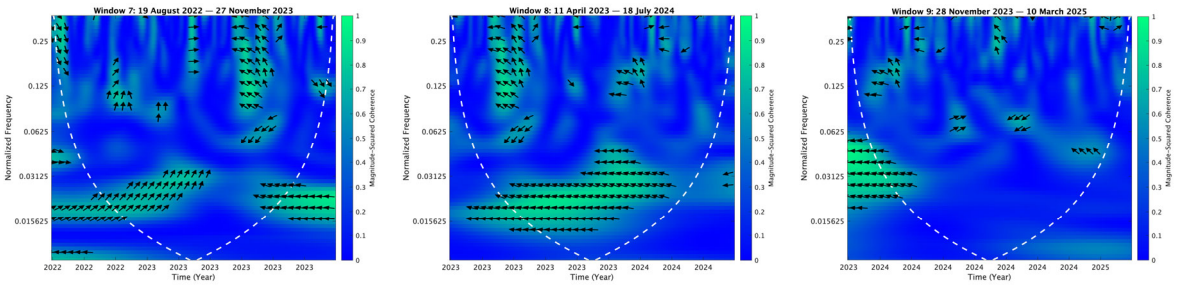

Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

CA

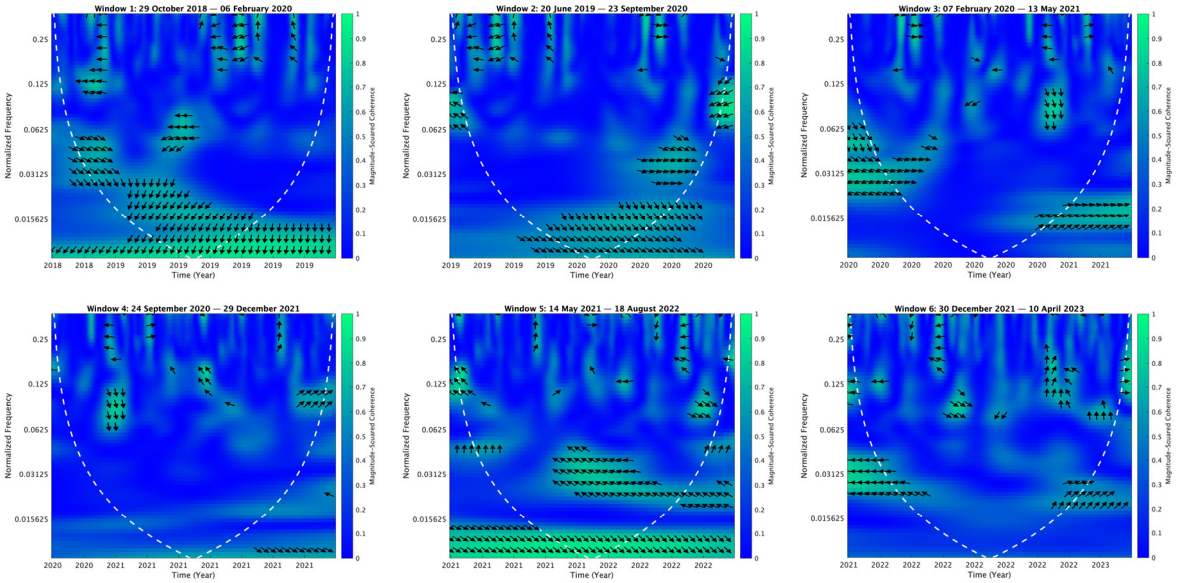

Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

SS

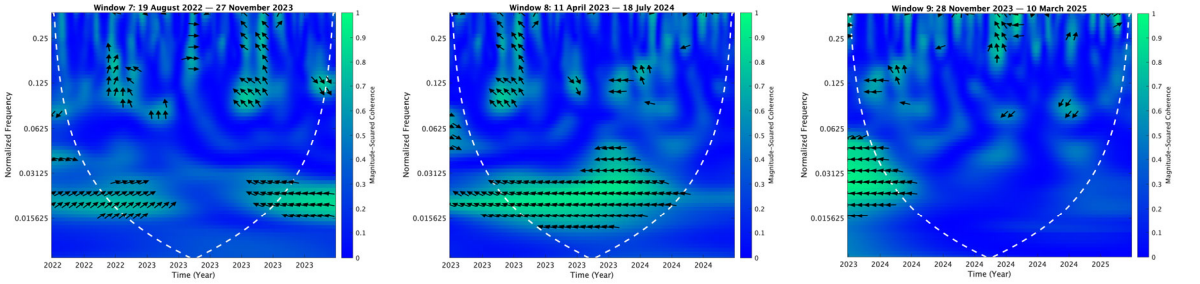

Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence


Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

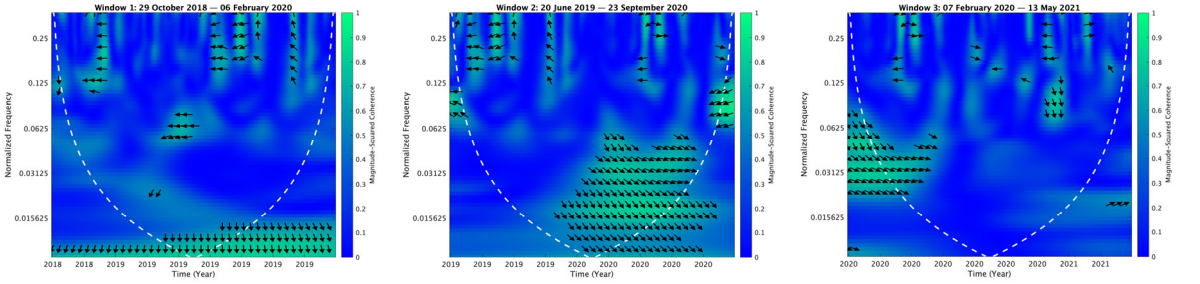
CI

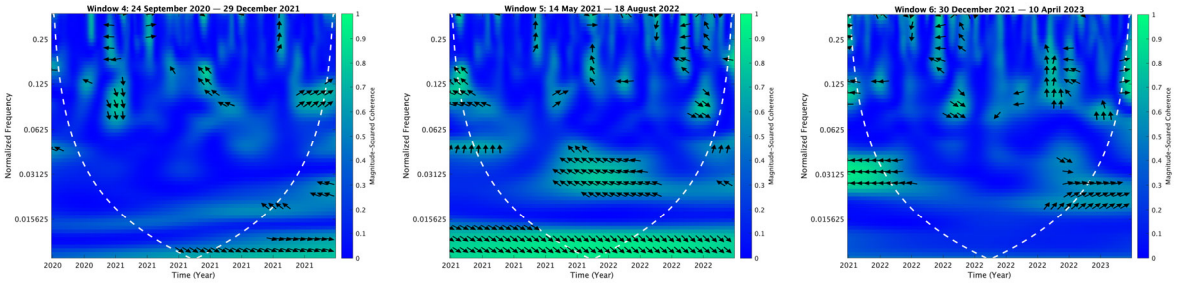

Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

QCLN

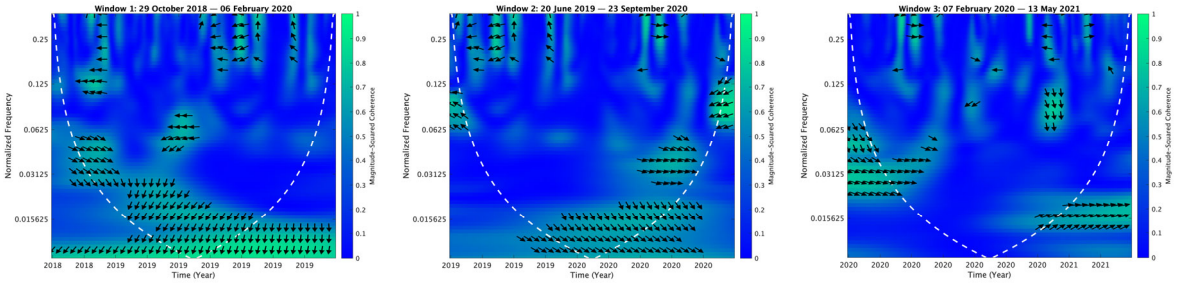

Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

CA


Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

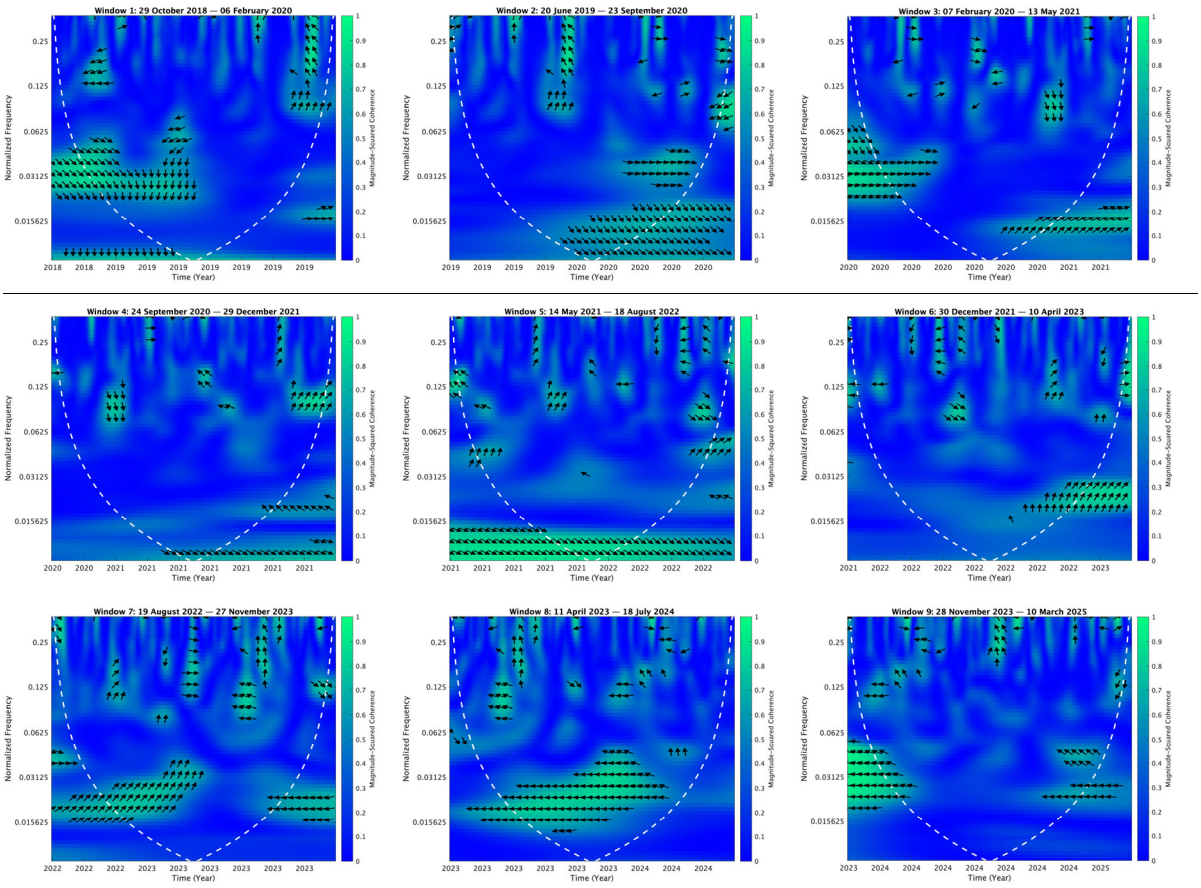

Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

SS

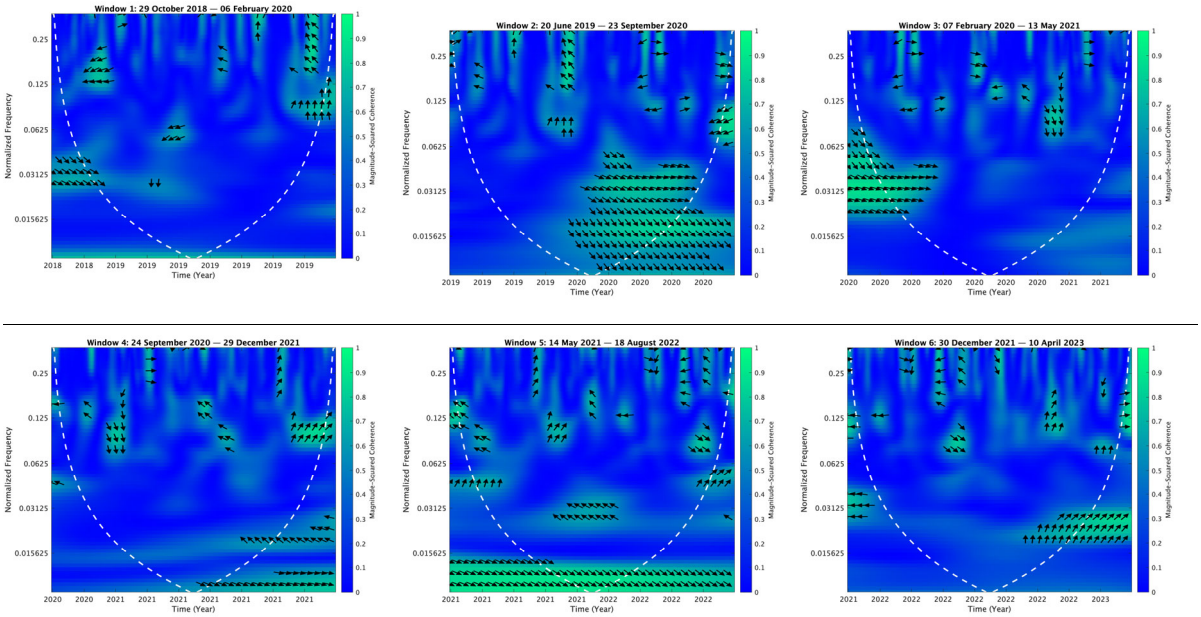

Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

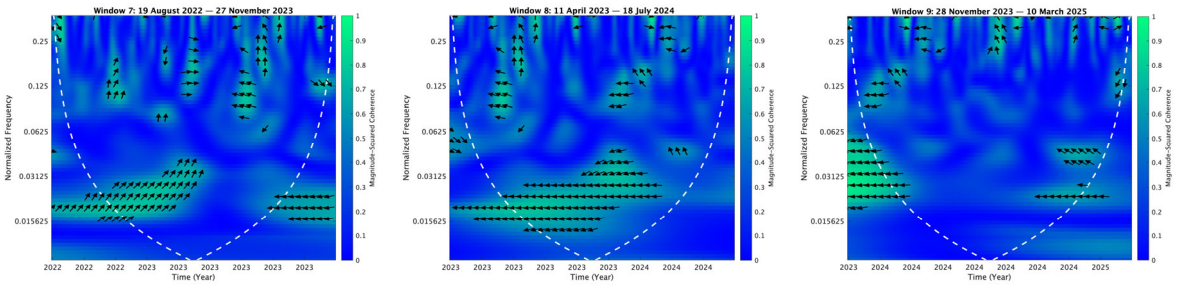
CI

CNRG

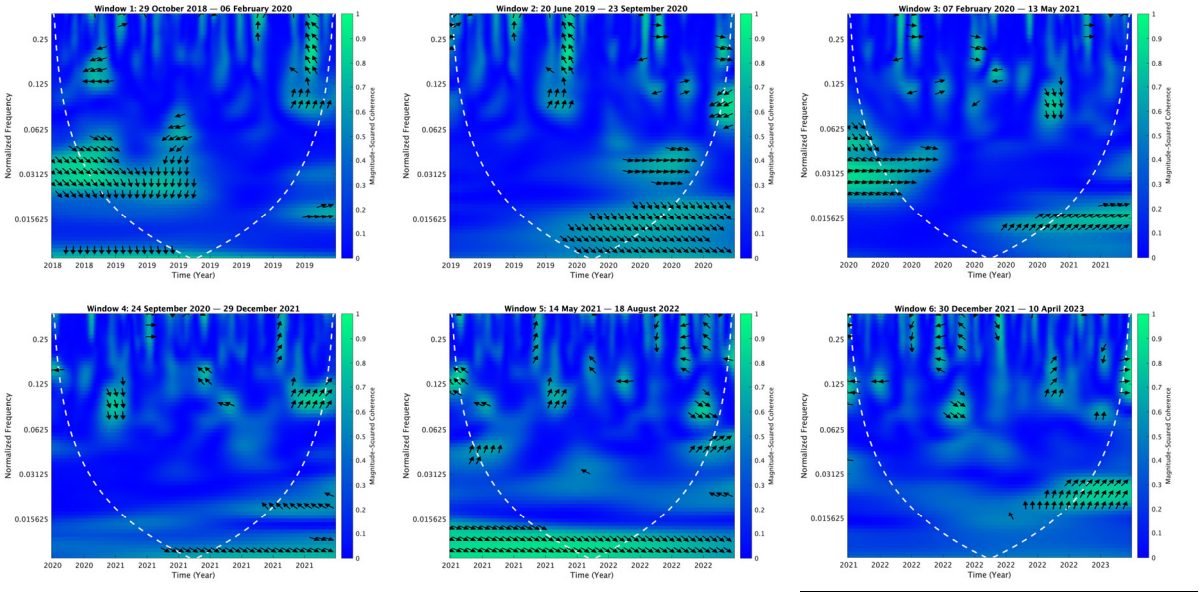

Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

CA


Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

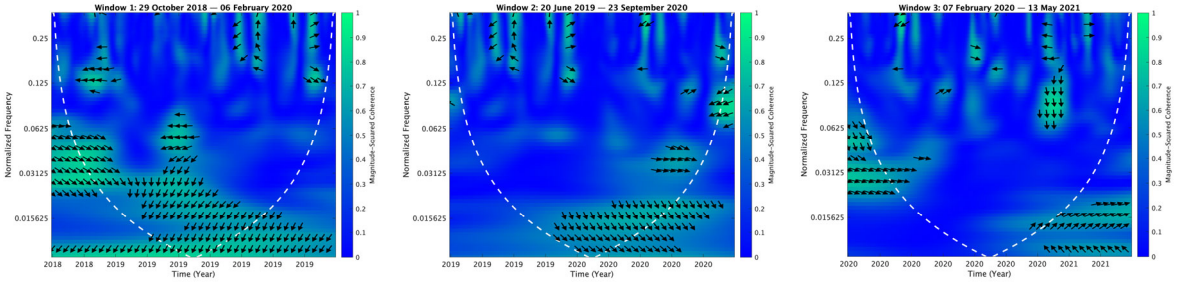

Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

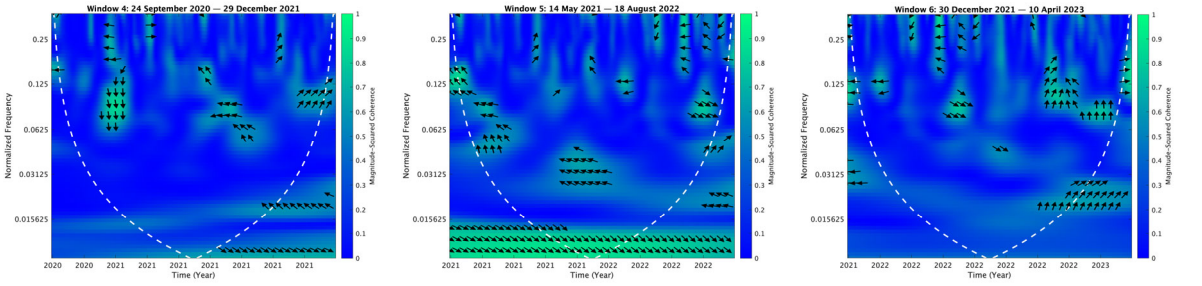
SS


Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

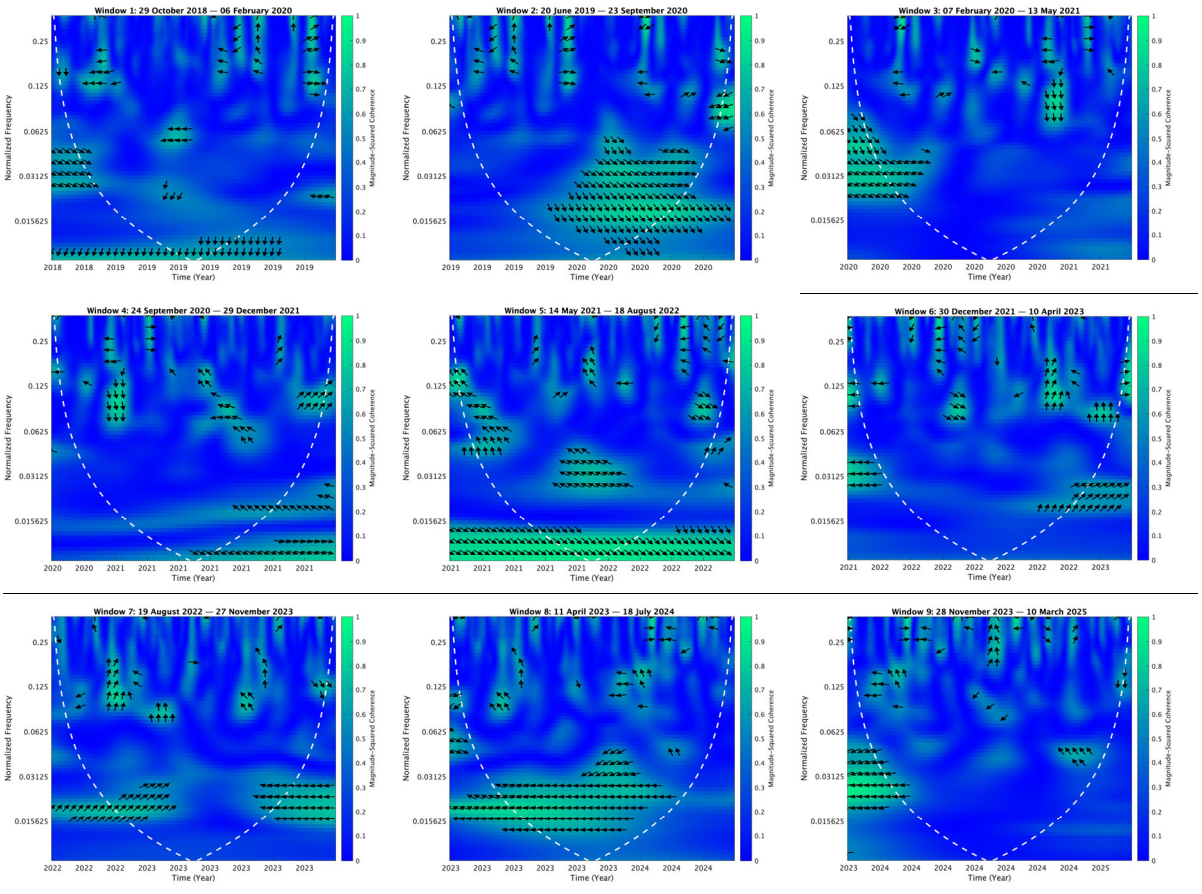
CI

ACES

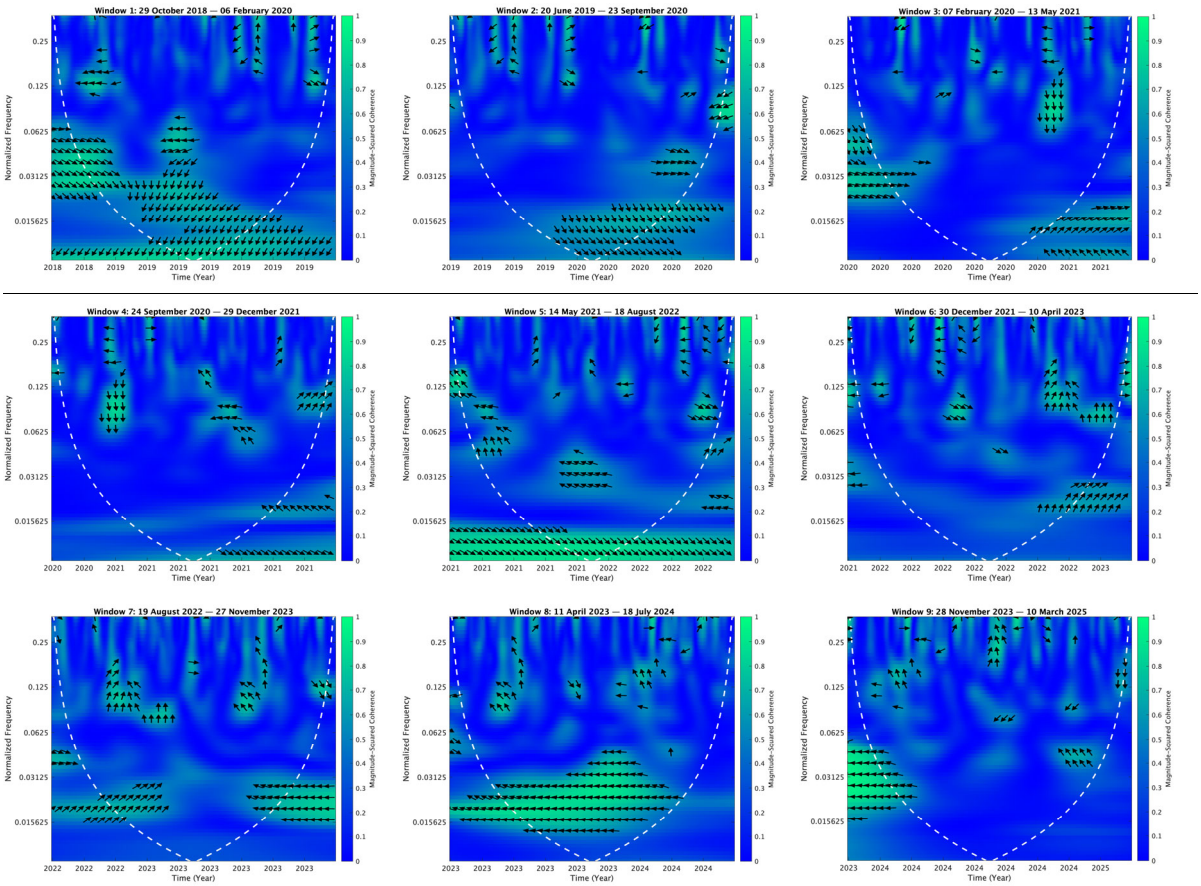

Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence


Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

CA

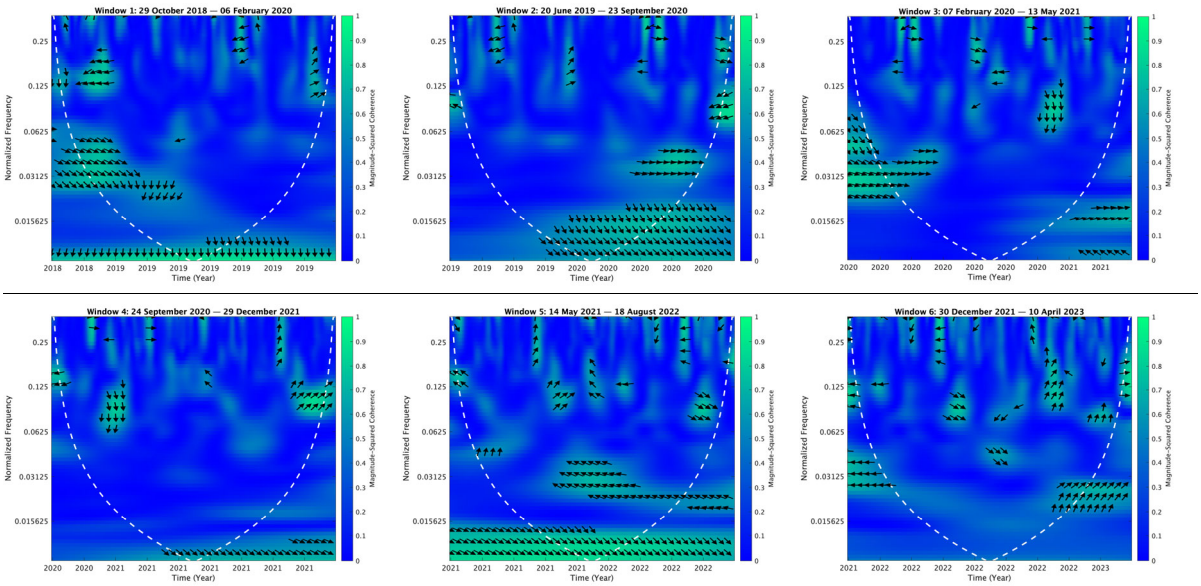

Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

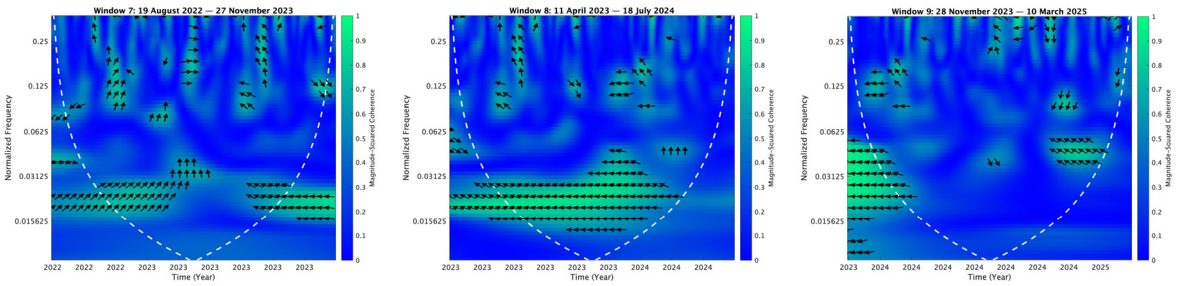
SS


Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

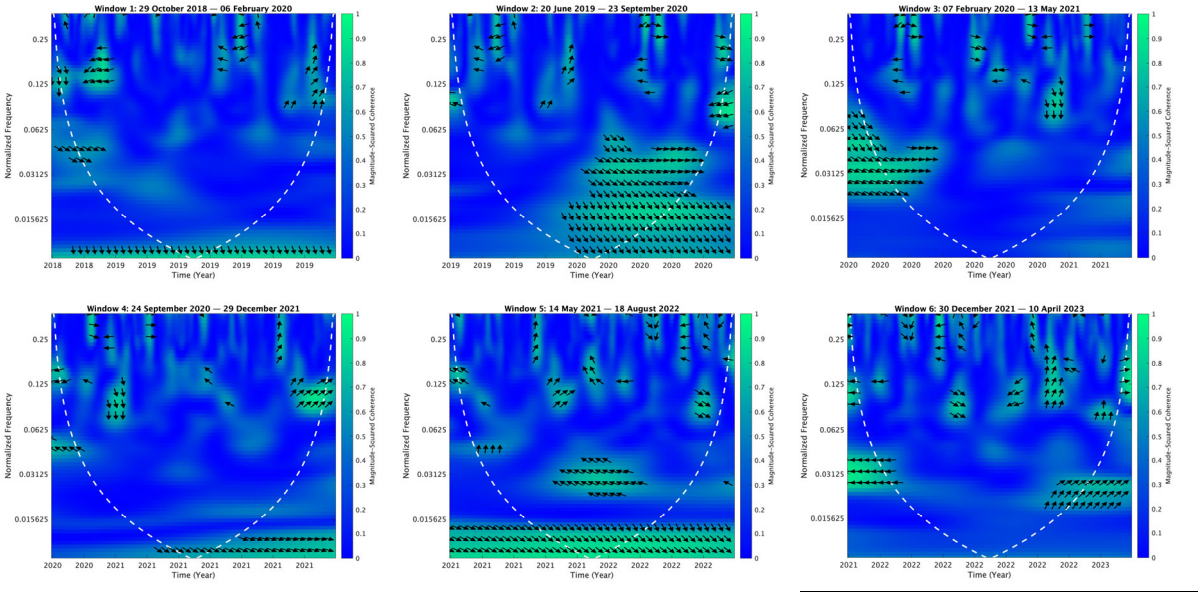
CI

PBW

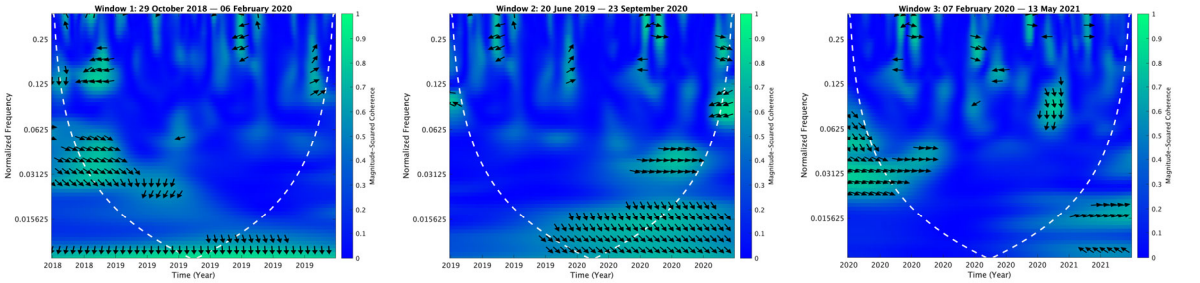

Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

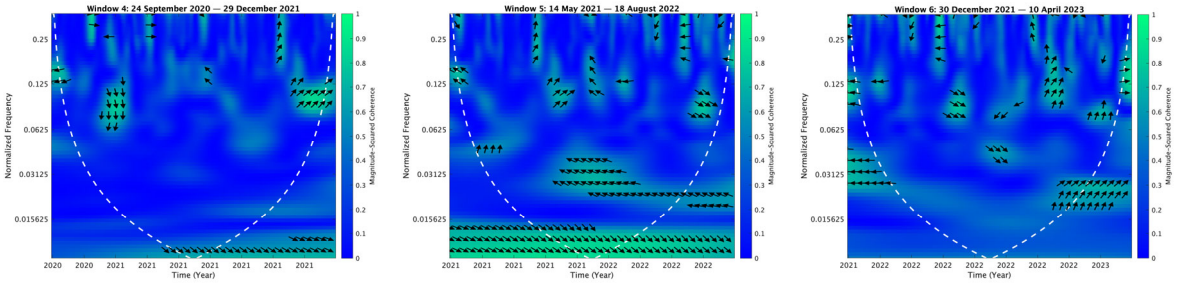

Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

CA

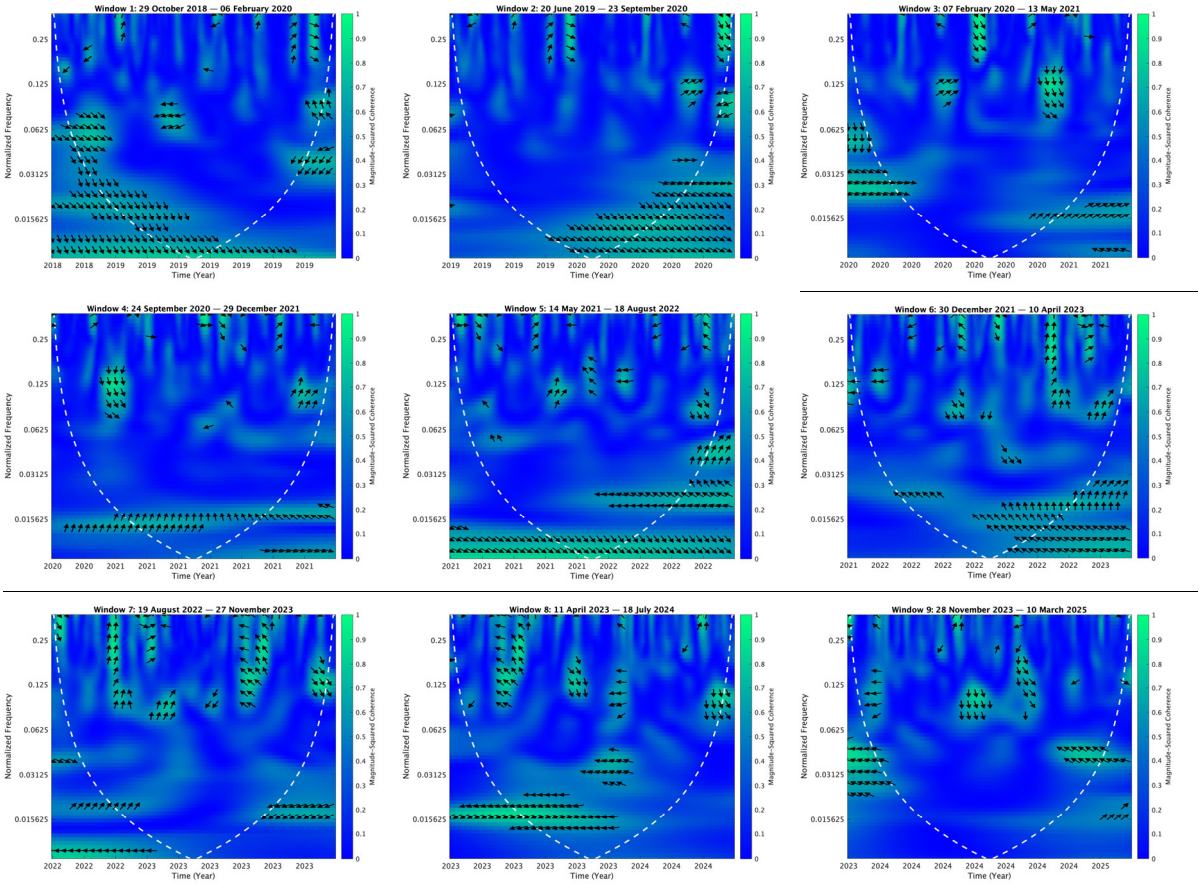

Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

SS


Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

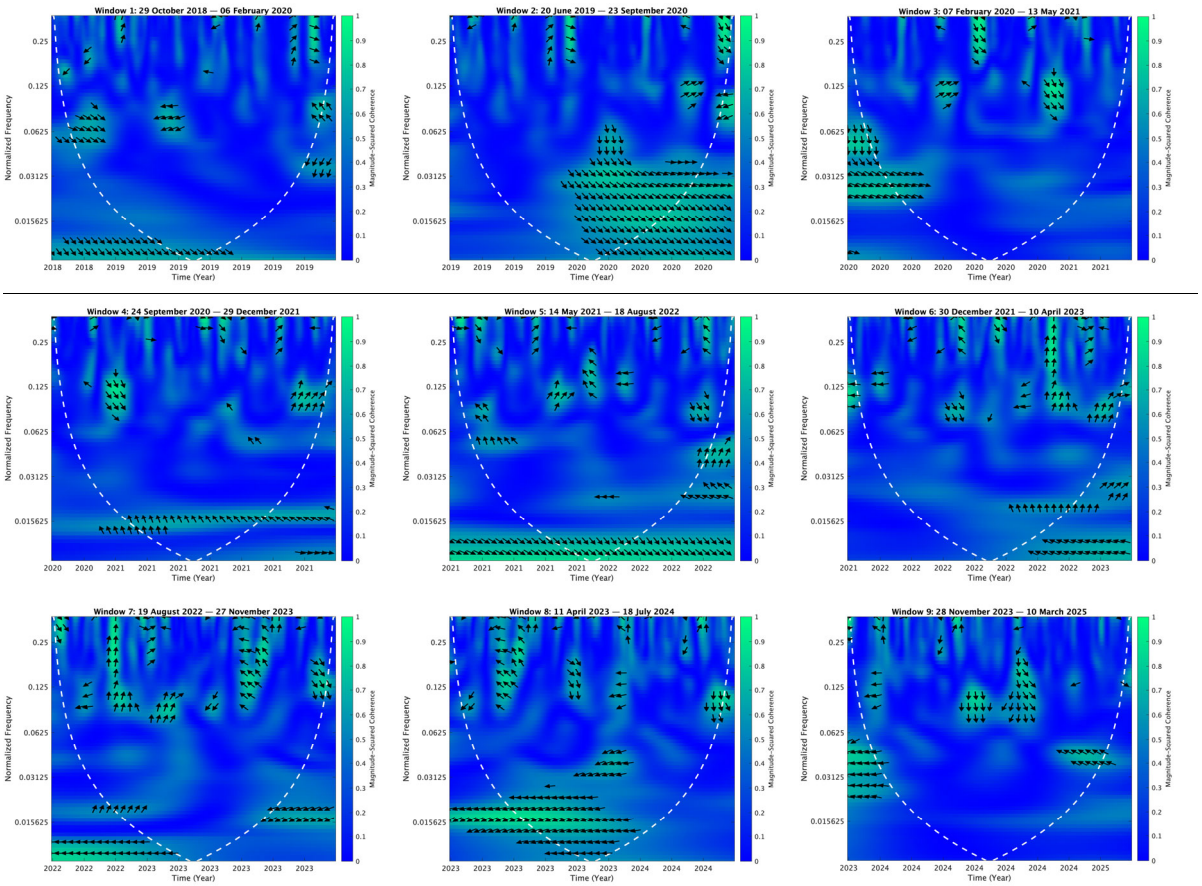

Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

CI

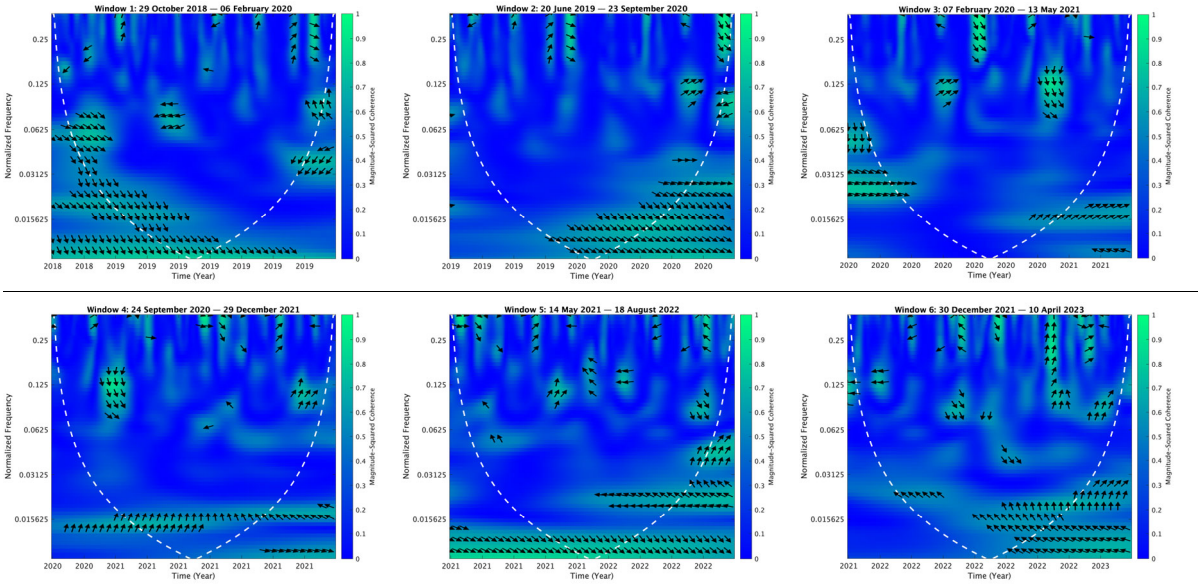

Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

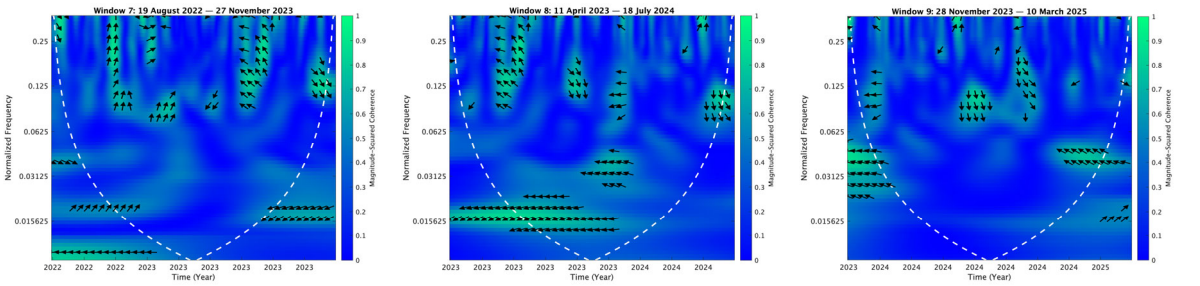
RNRG

CA

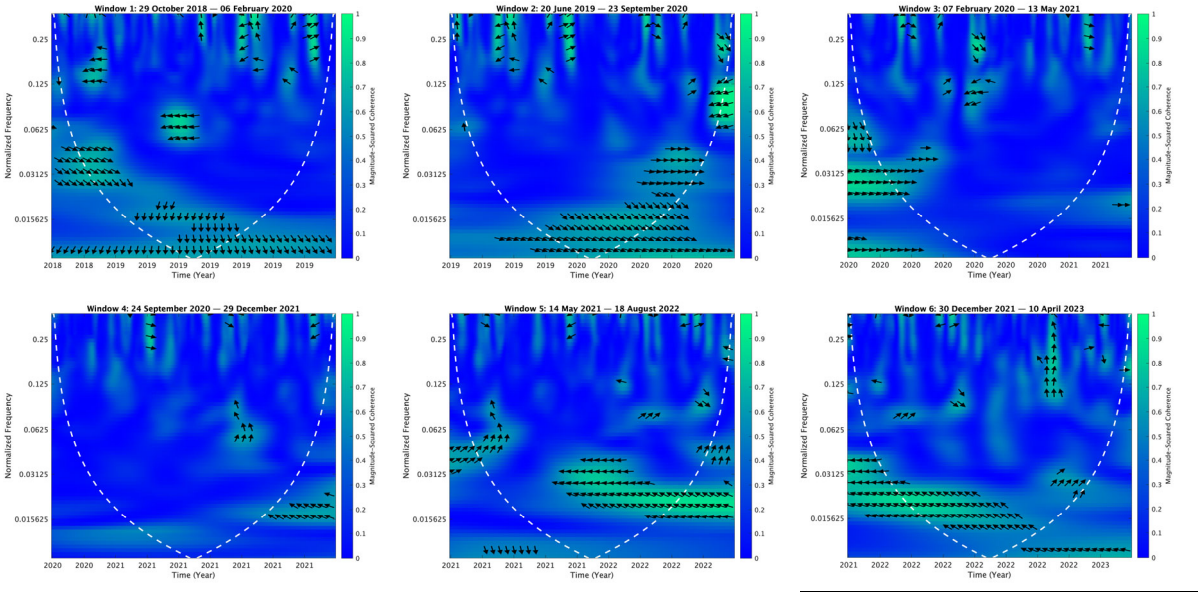

Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

SS

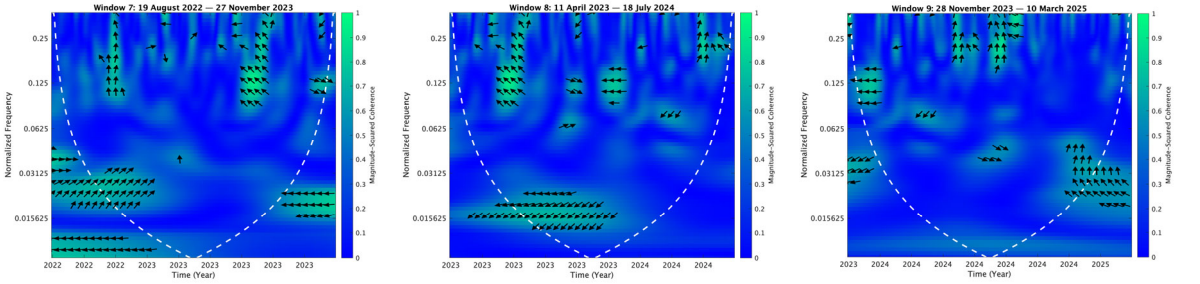

Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence


Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

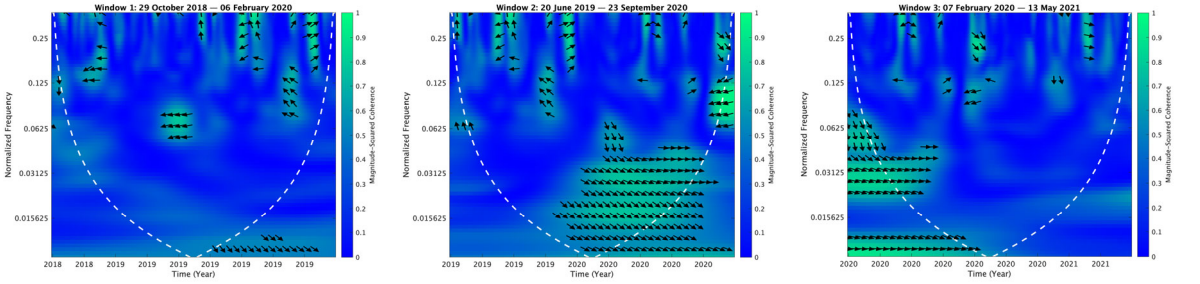
CI

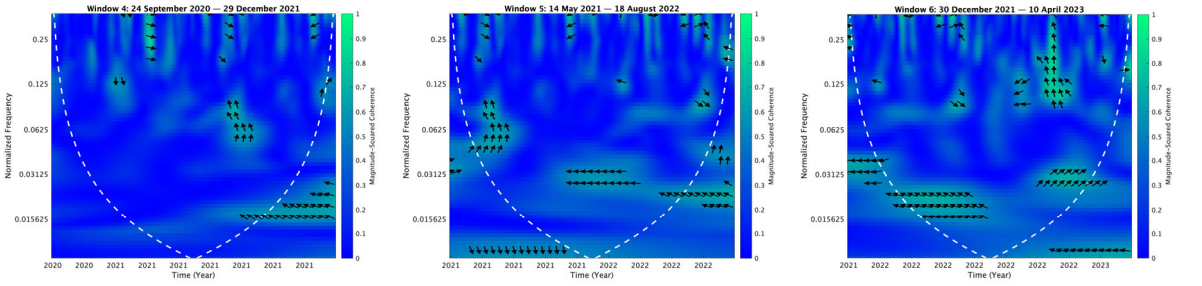

Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

ACWI

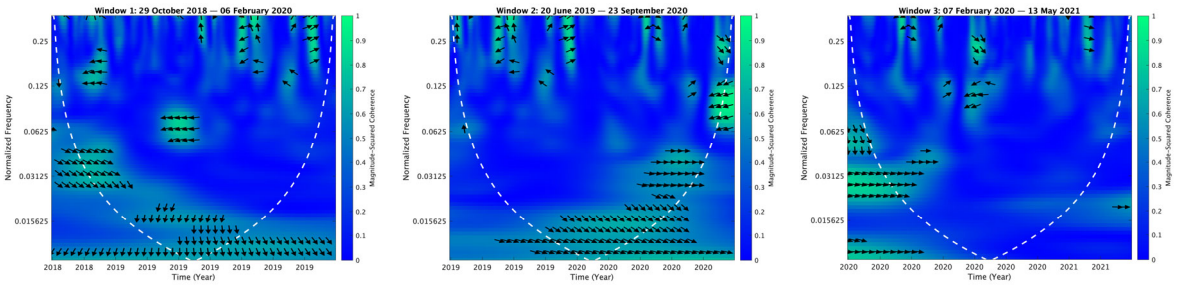

Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

CA


Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

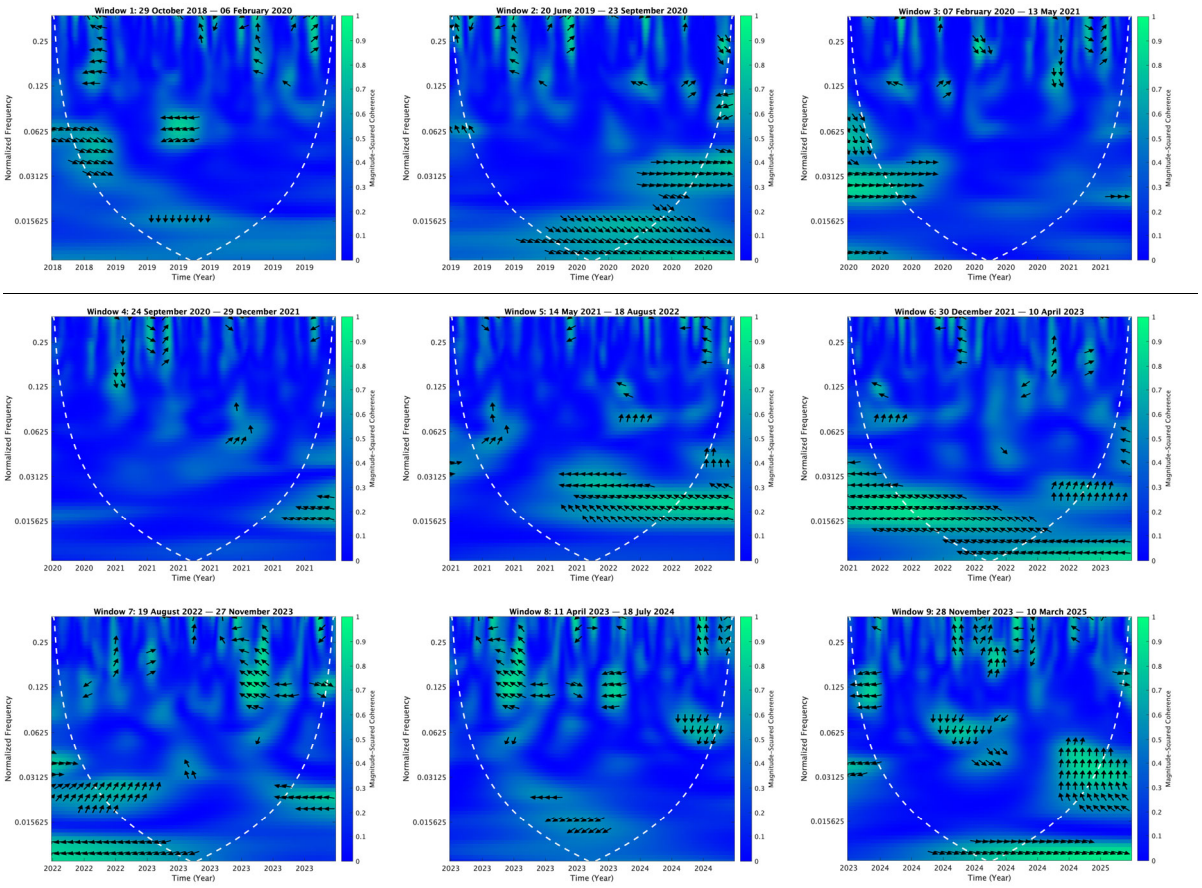

Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

SS

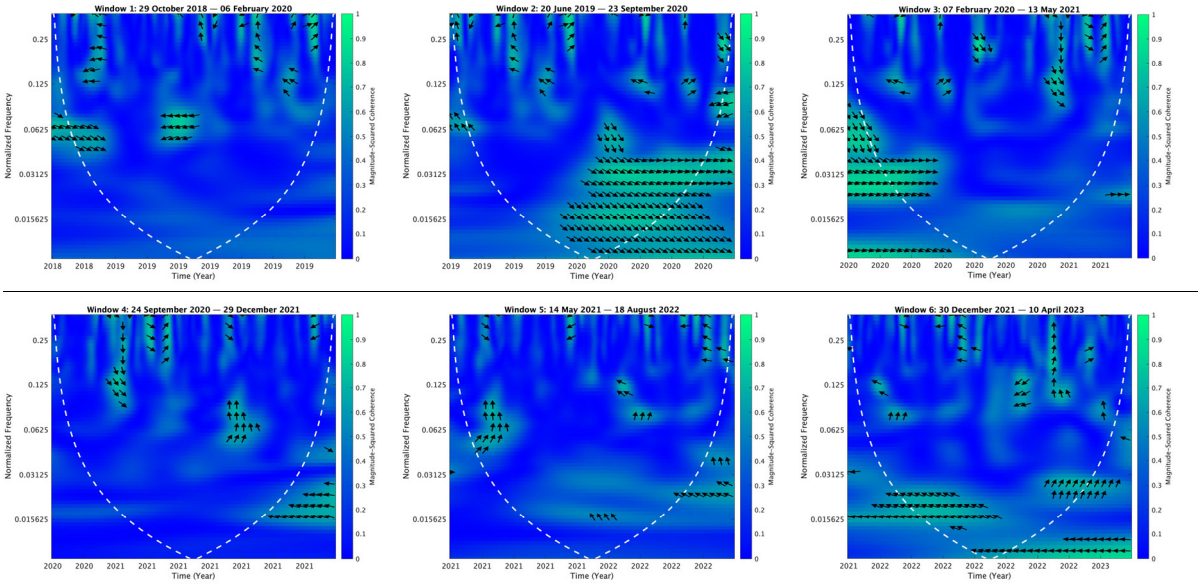

Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

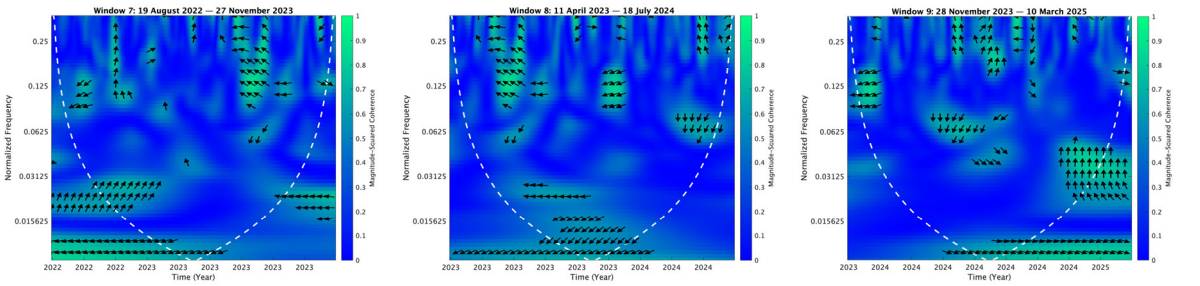
CI

IEUR

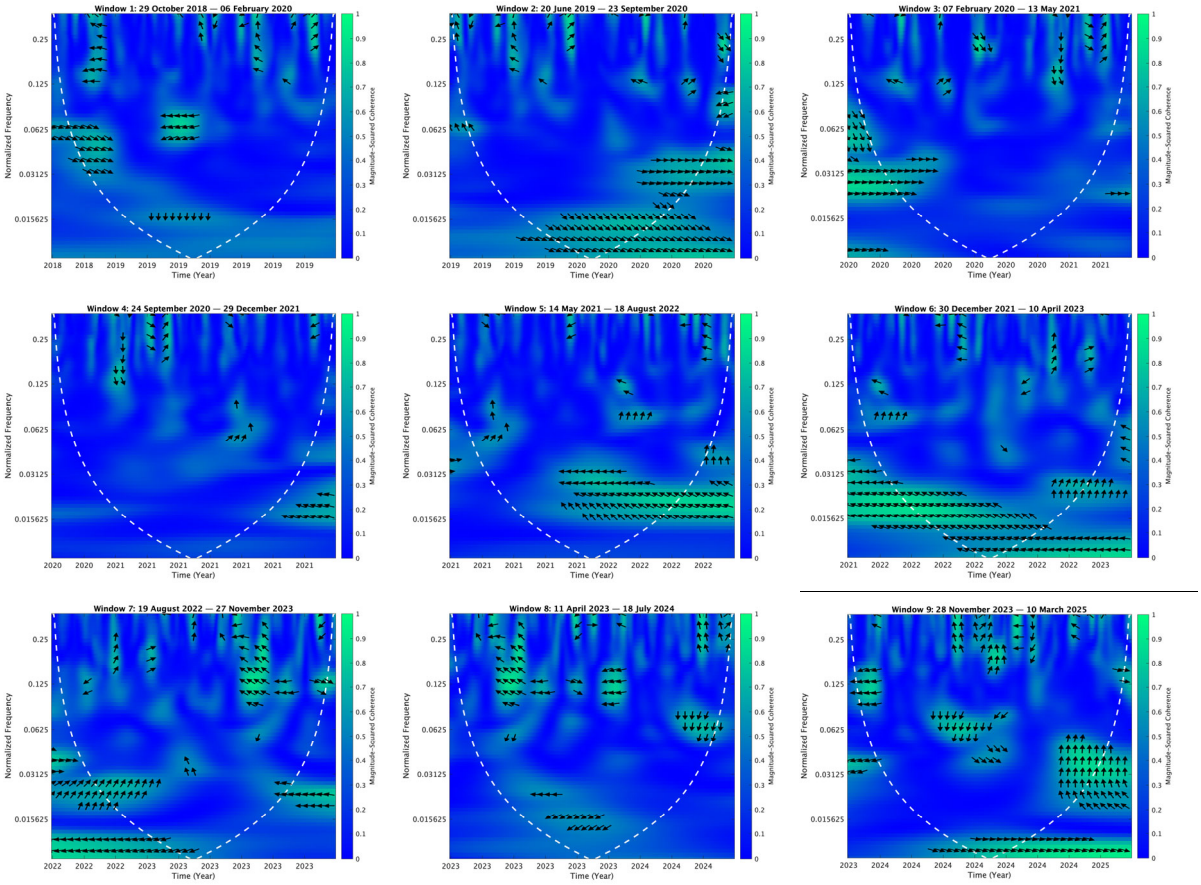

Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

CA


Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

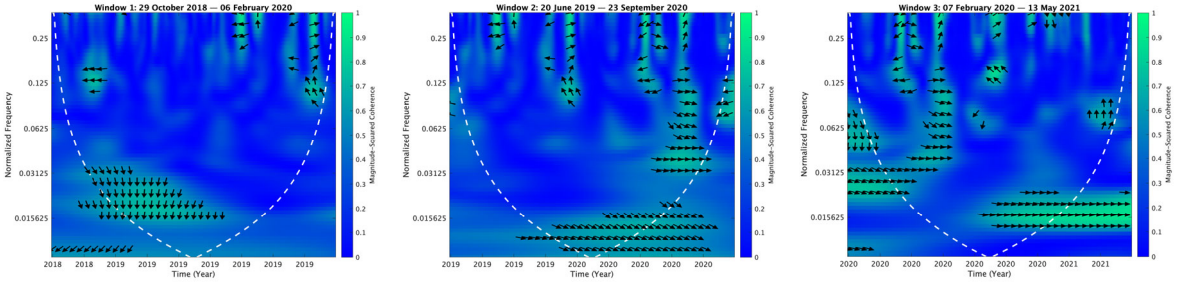

Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

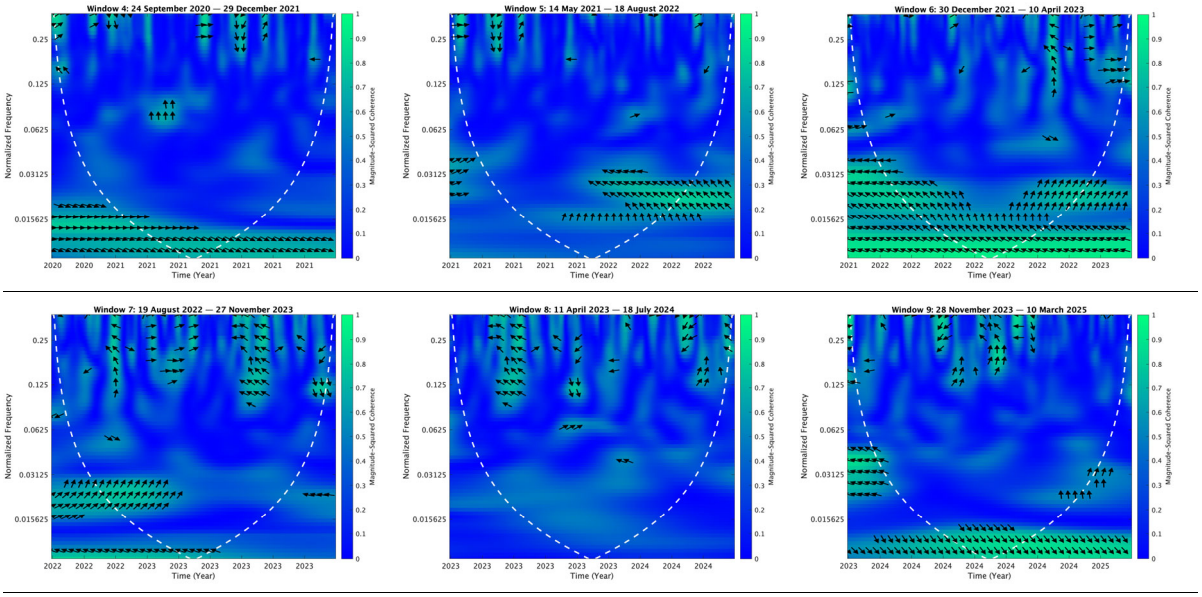
SS


Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

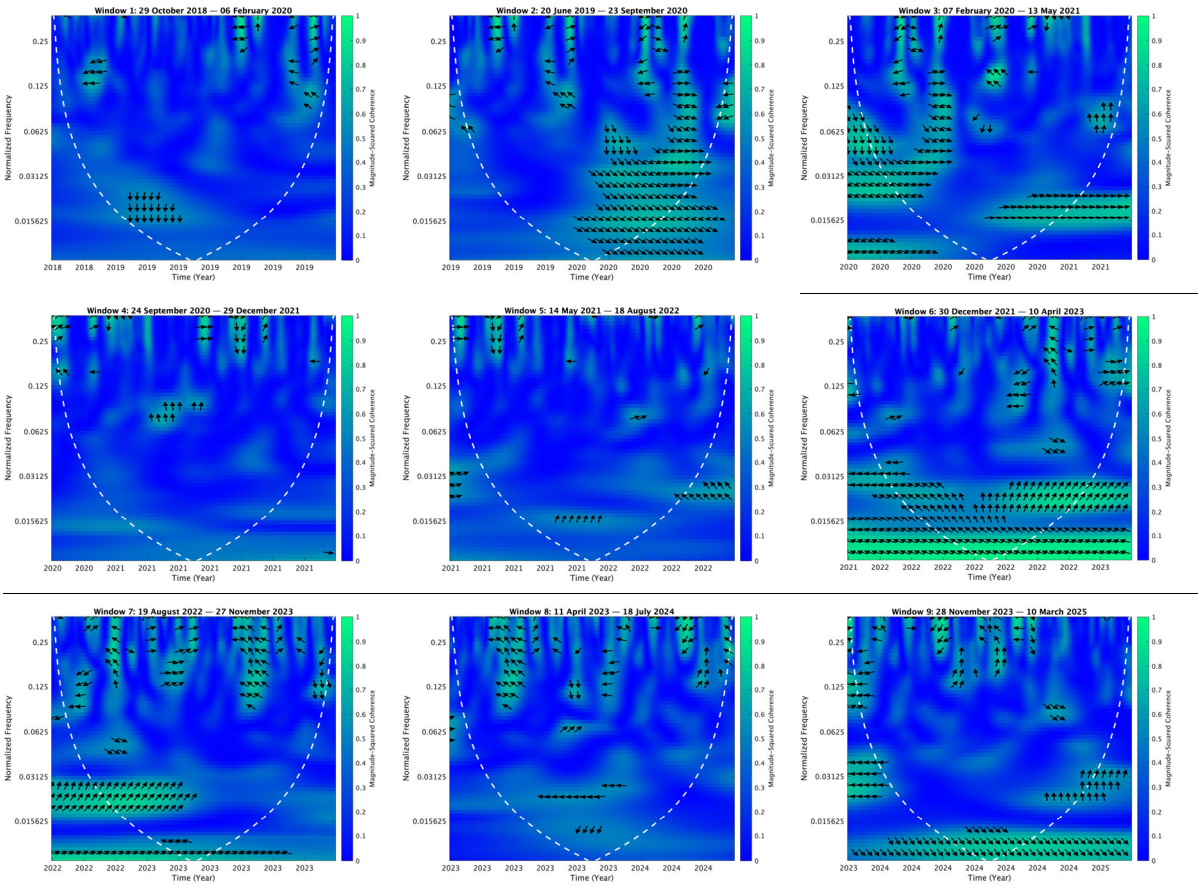
CI

EEMA

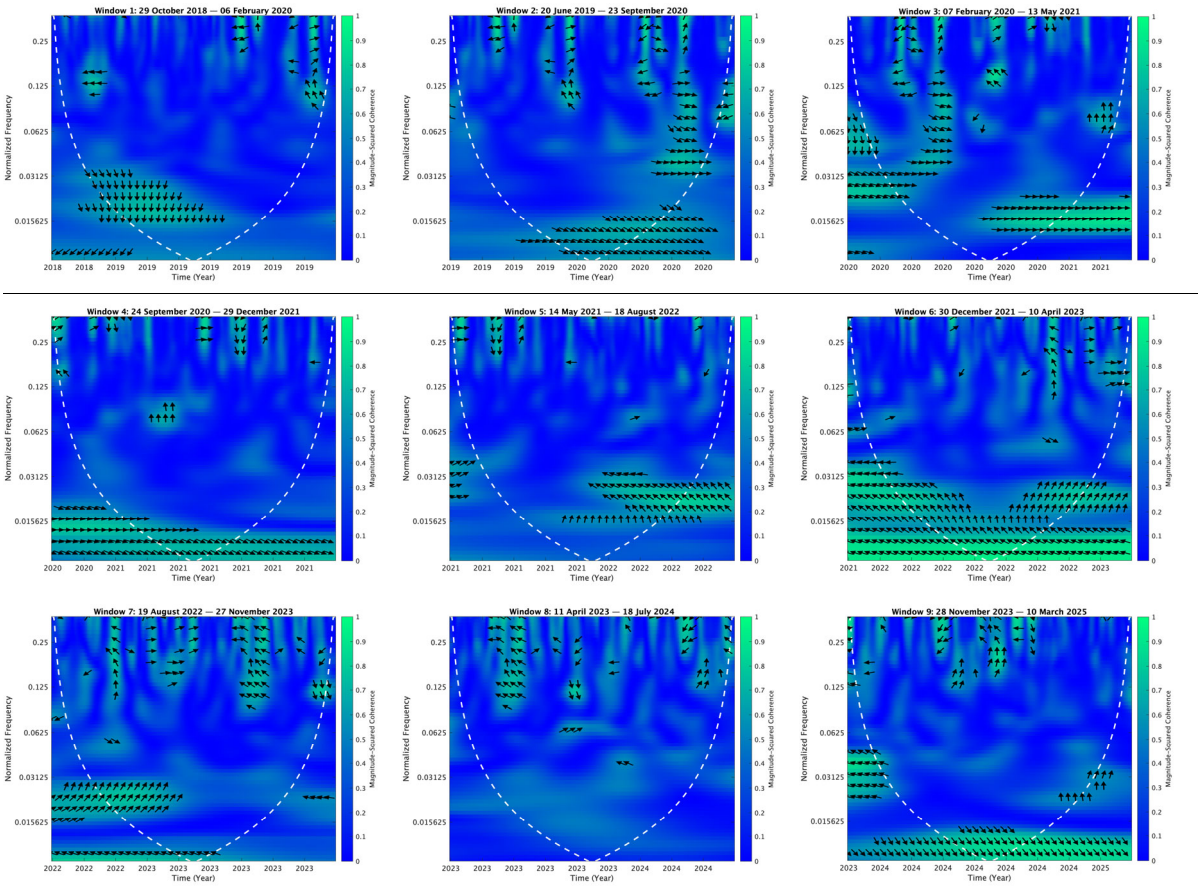

Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence


Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

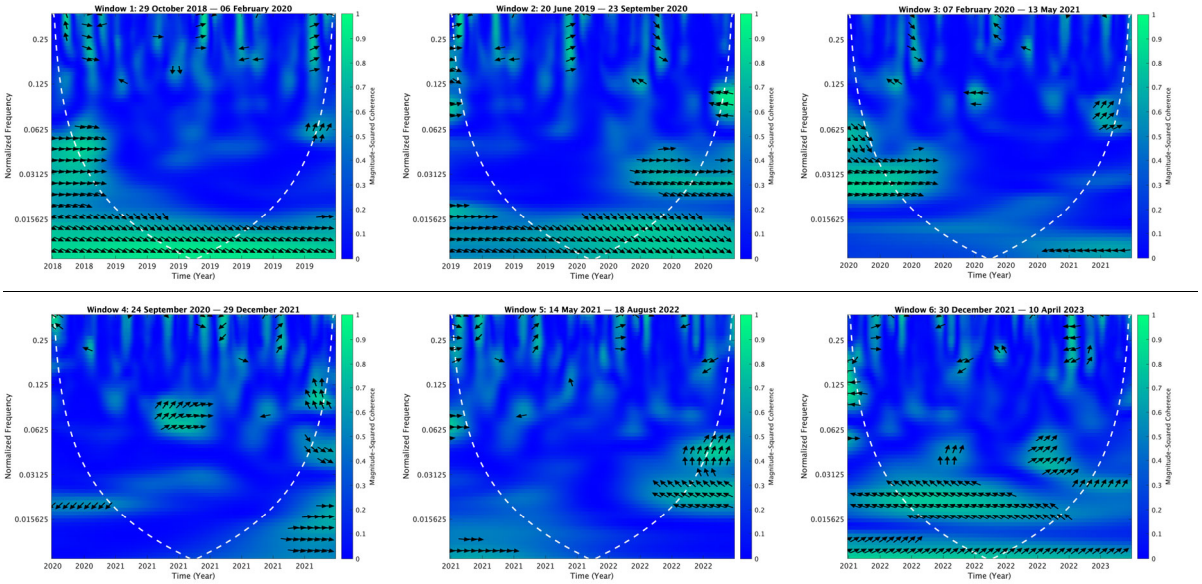
CA


Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

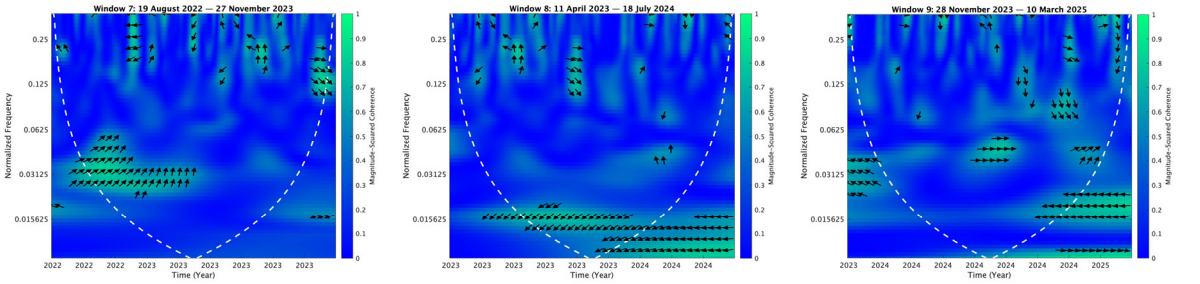
SS


Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

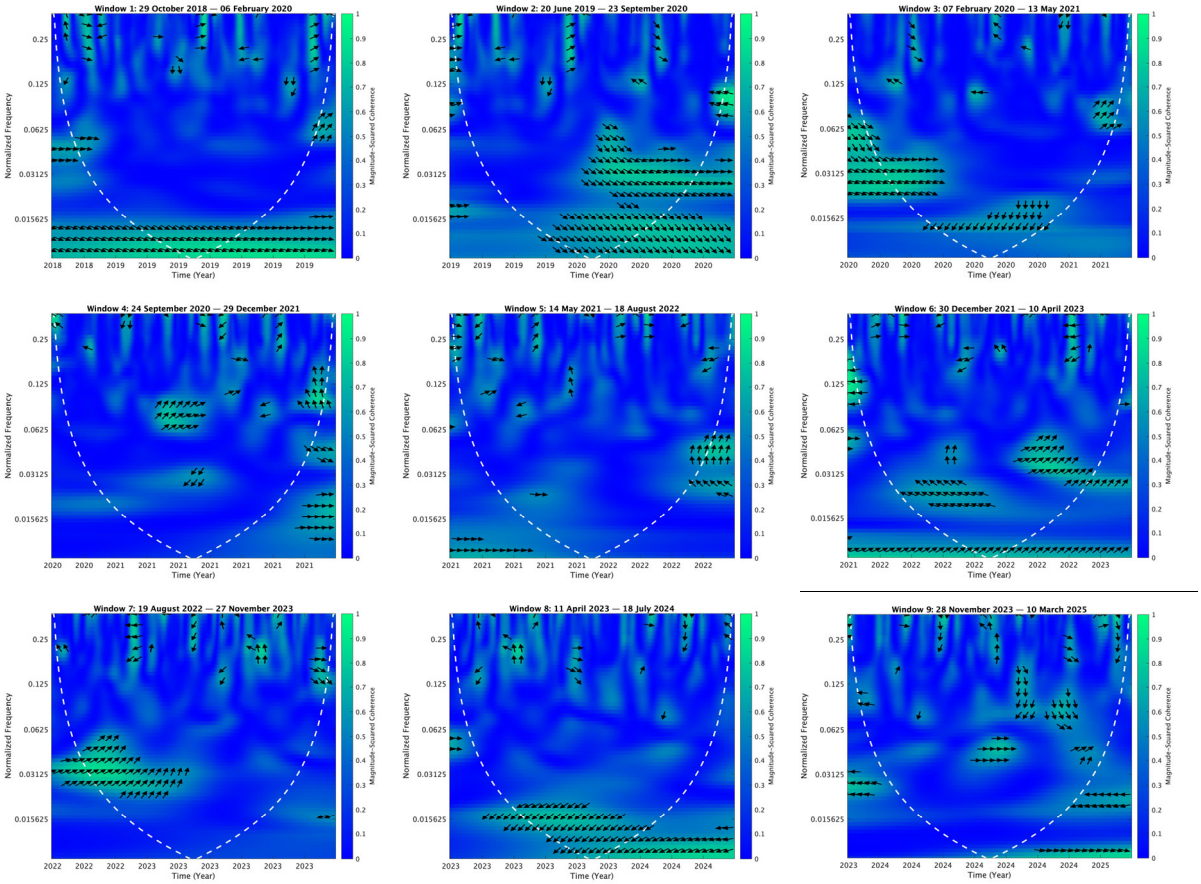
CI


Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

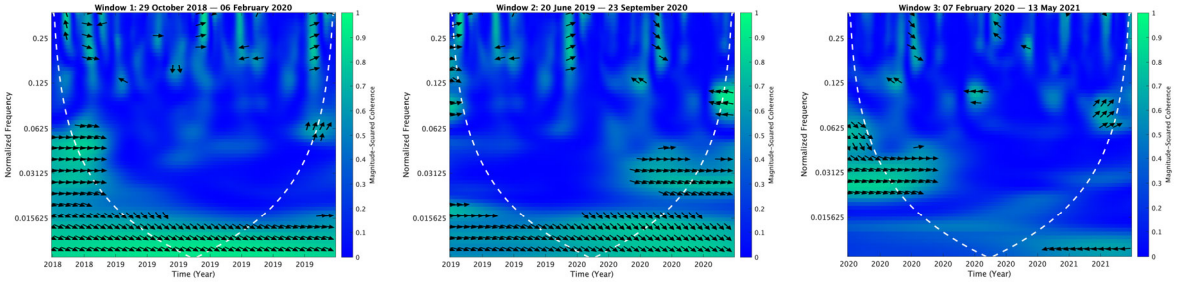
EWZ

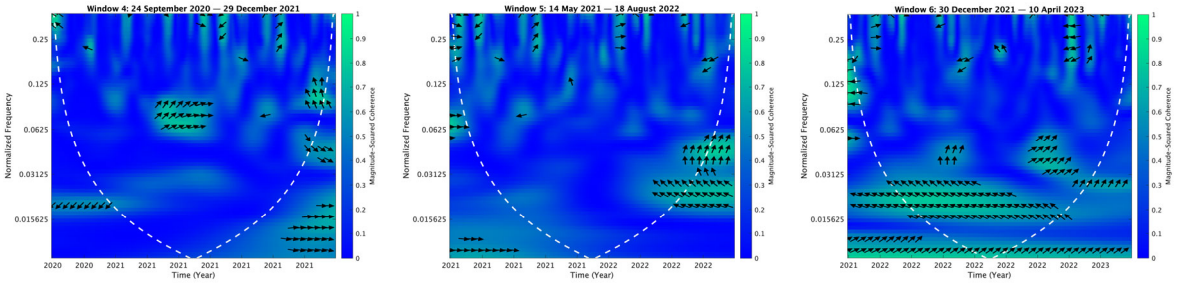

Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

CA


Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

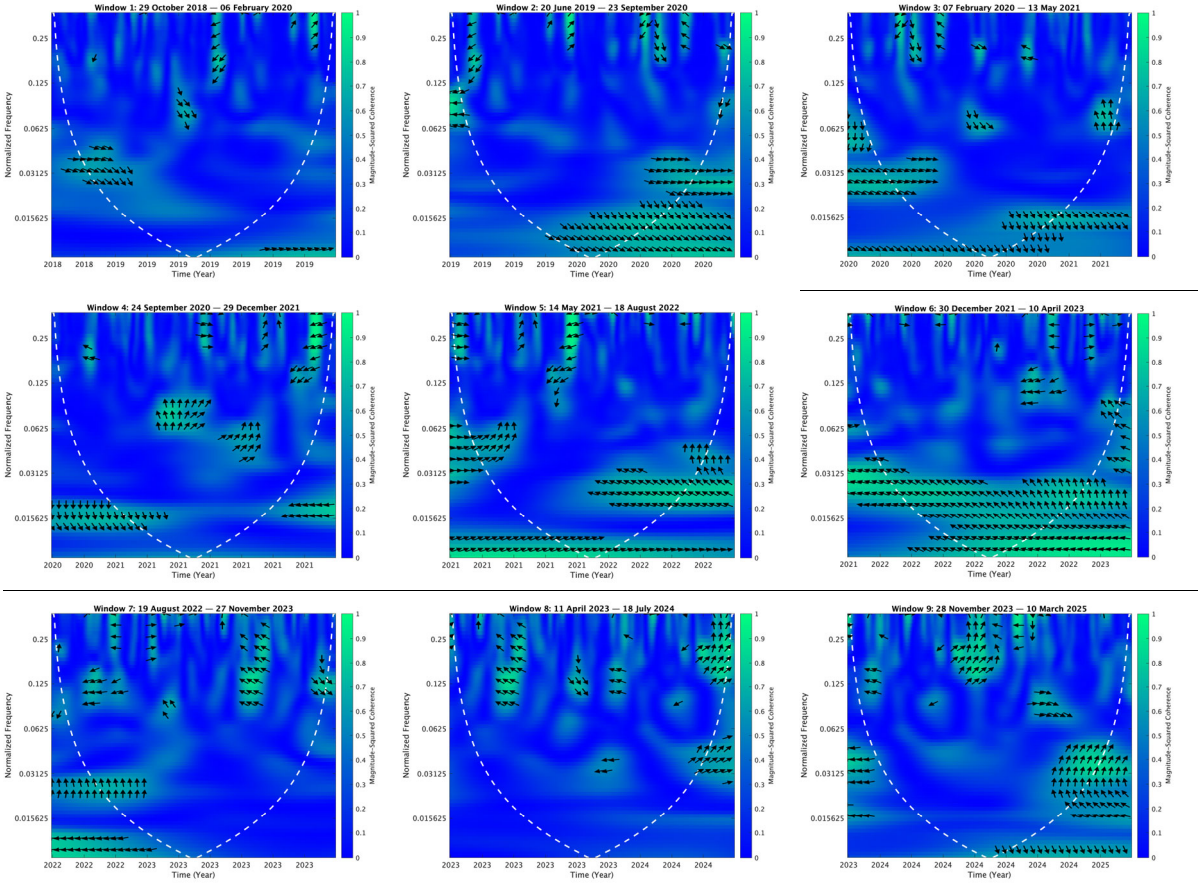
SS


Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

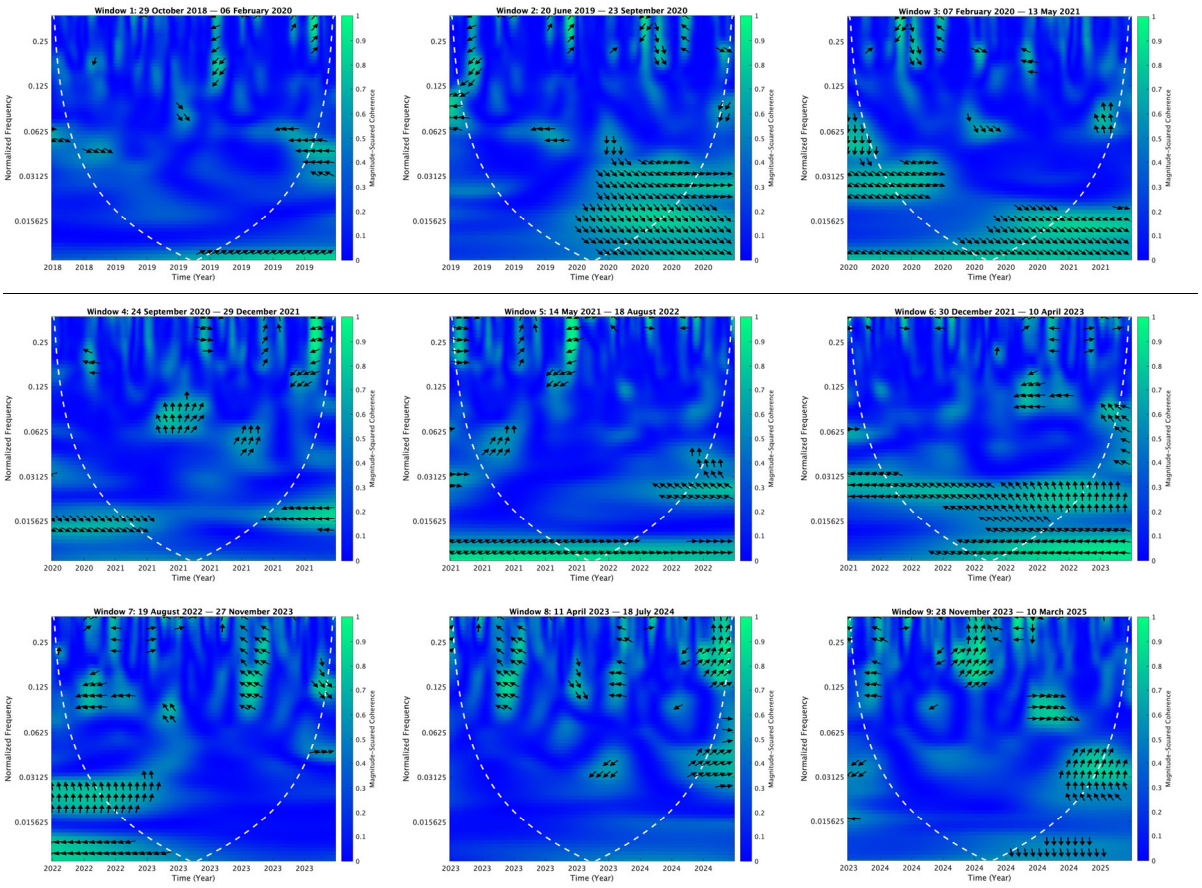

Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

CI

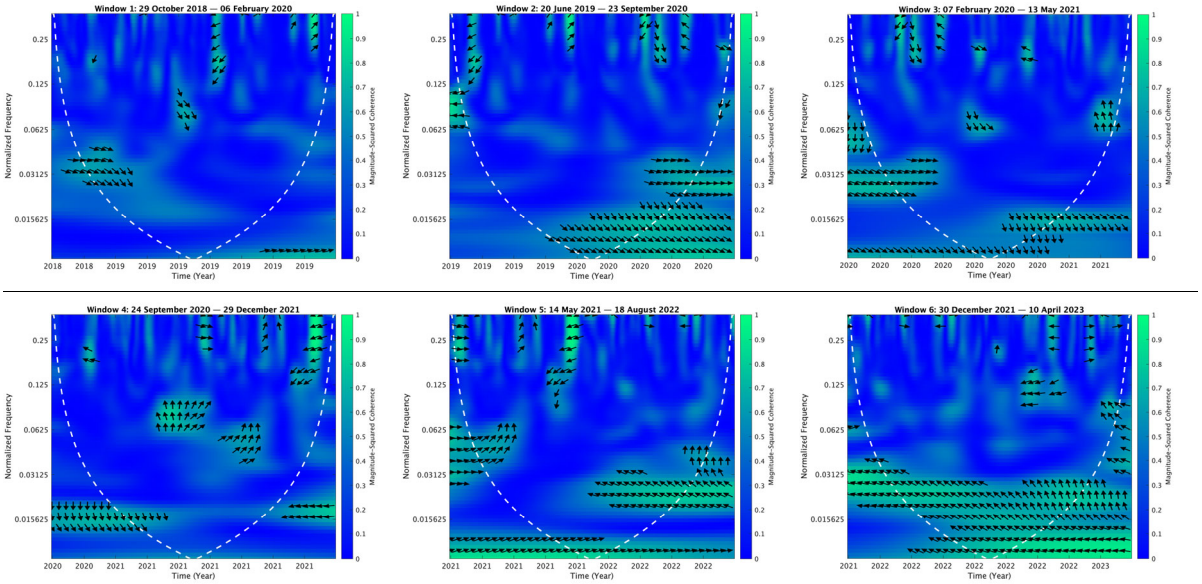
EZA

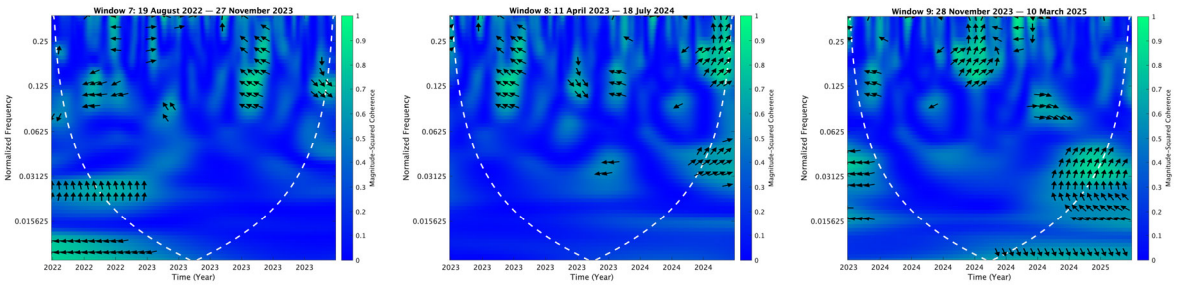

Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

CA

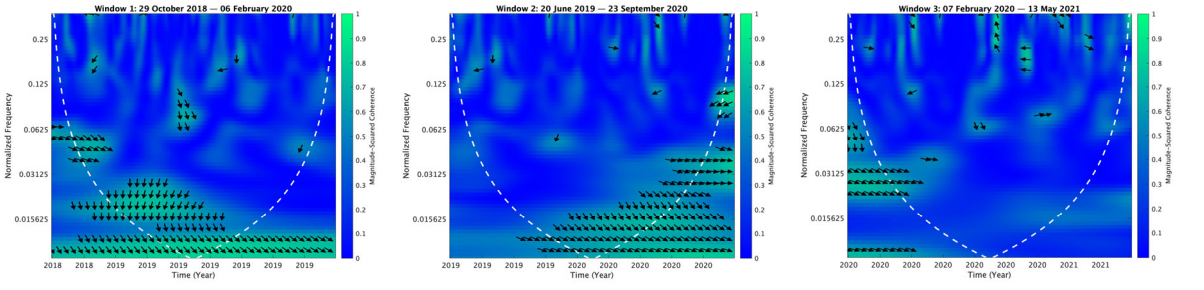

Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

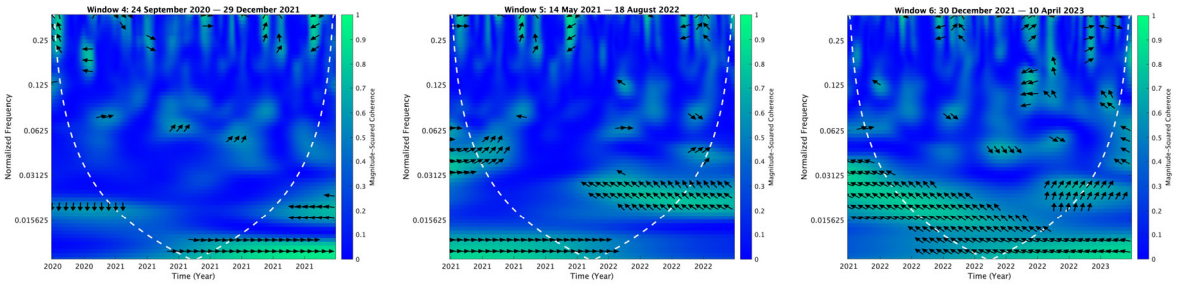
SS


Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

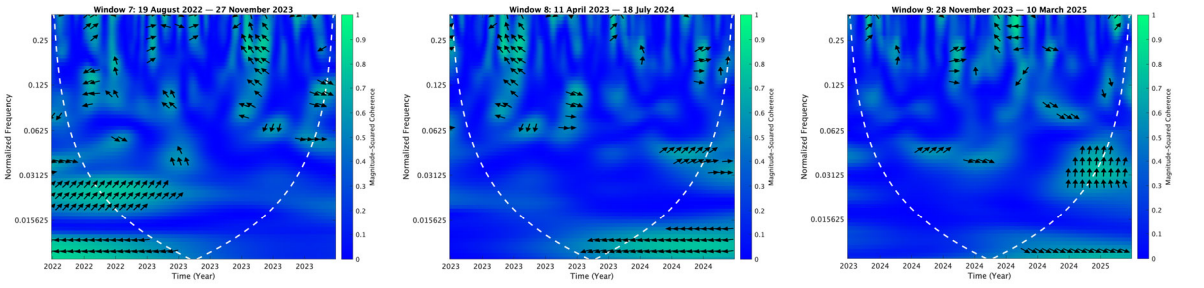

Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

CI

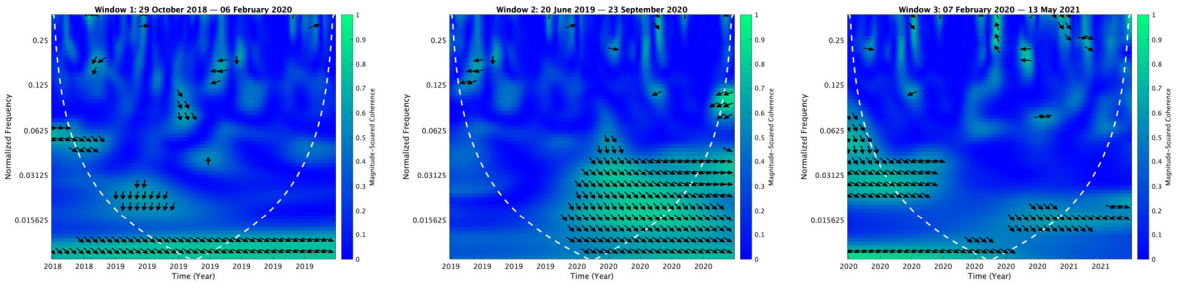

Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

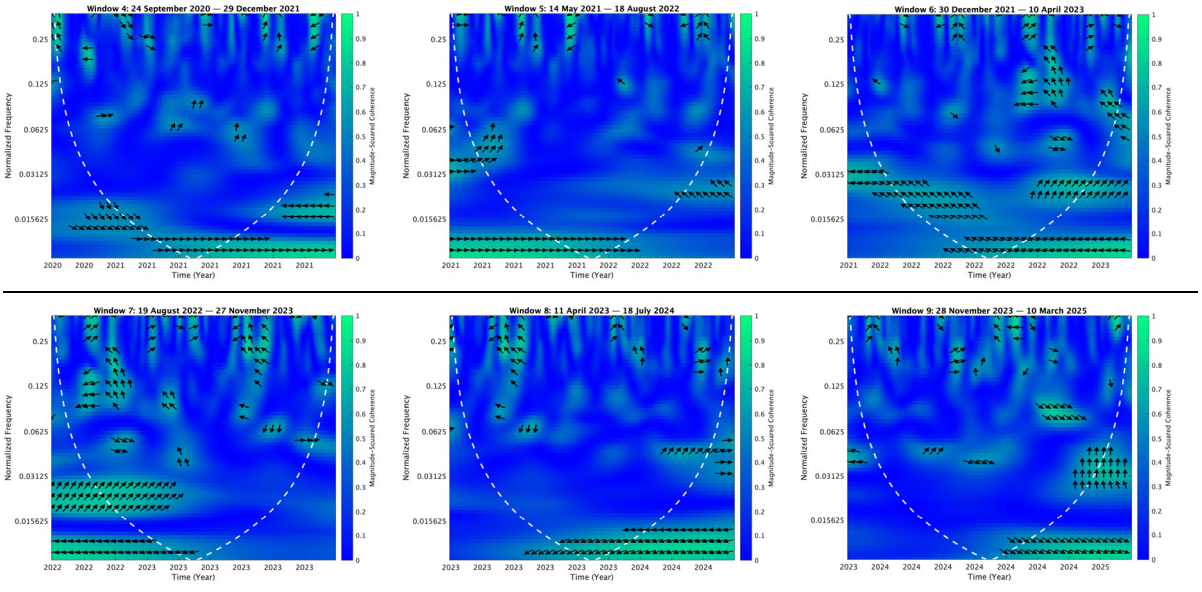

Window 4: 24 September 2020 — 29 December 2021
Window 5: 14 May 2021 — 18 August 2022
Window 6: 30 December 2021 — 10 April 2023
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

AFK

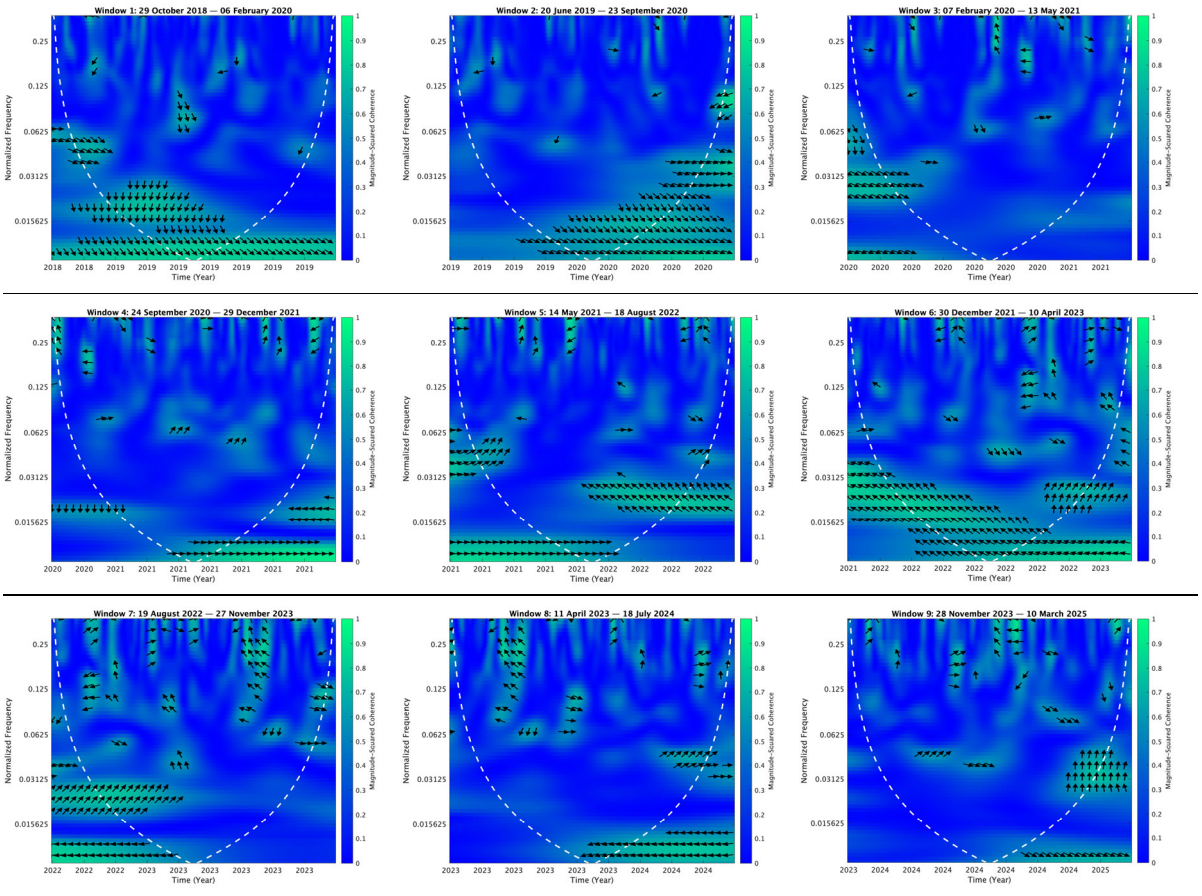

Window 7: 19 August 2022 — 27 November 2023
Window 8: 11 April 2023 — 18 July 2024
Window 9: 28 November 2023 — 10 March 2025
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence

CA


Window 1: 29 October 2018 — 06 February 2020
Window 2: 20 June 2019 — 23 September 2020
Window 3: 07 February 2020 — 13 May 2021
Normalized Frequency
Time (Year)
Magnitude-Squared Coherence



SS

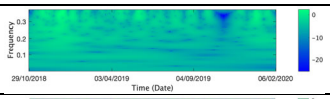
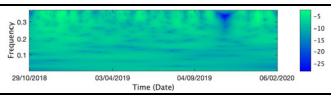
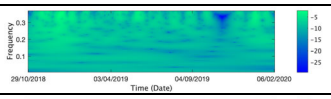
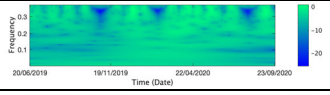
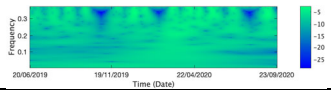
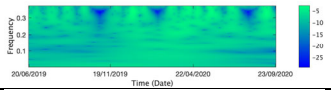
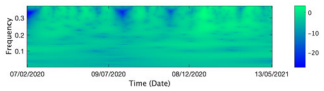
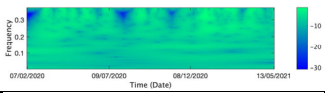
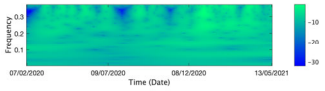
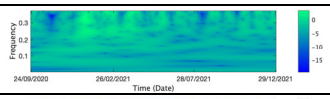
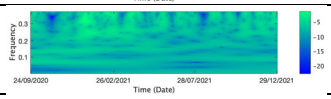
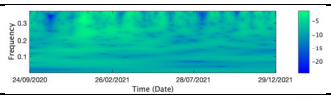
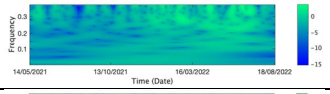
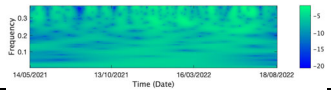
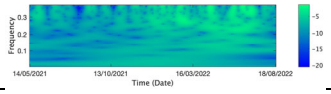
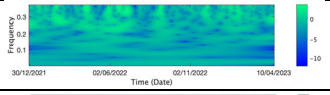
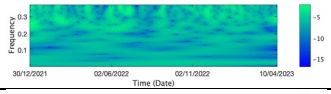
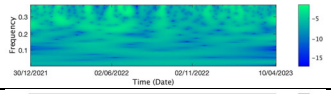
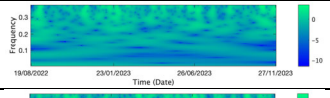
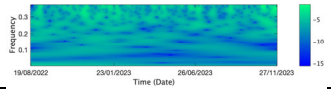
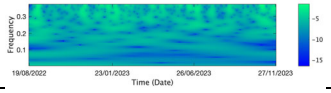
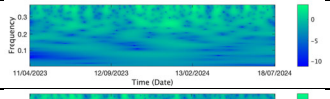
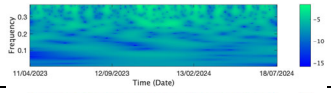
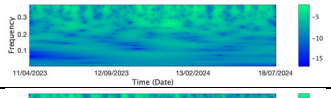
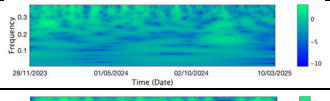
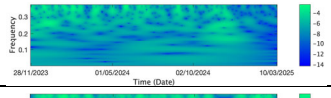
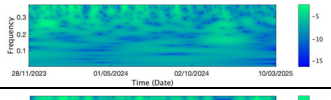
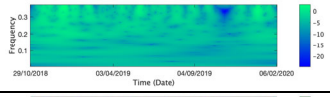
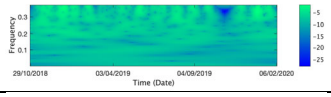
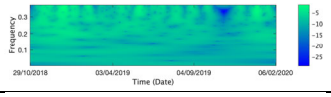
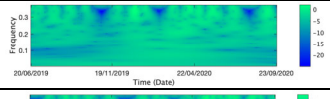
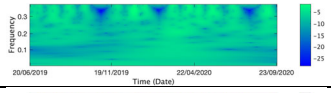
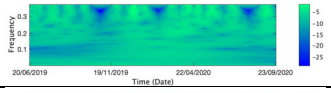
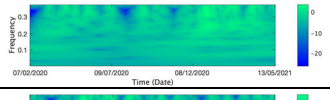
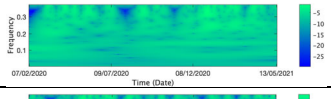
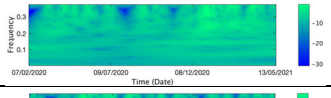
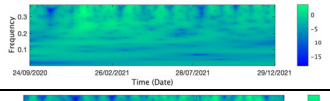
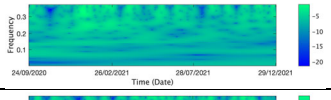
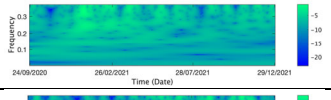
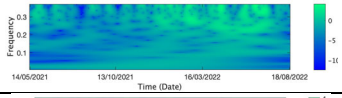


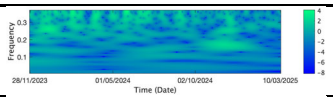
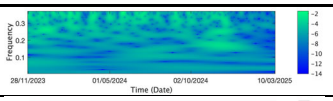
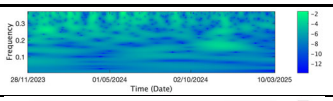
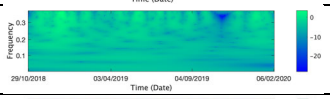
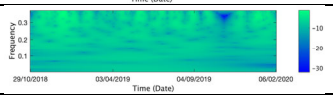
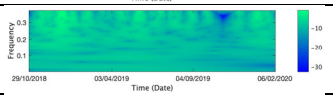
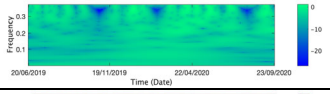
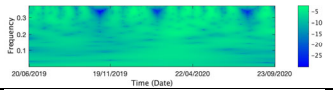
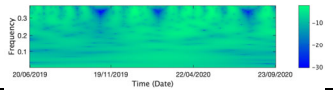
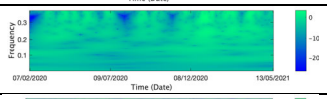
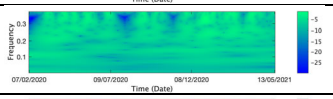
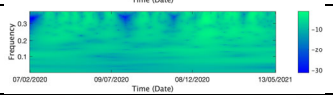
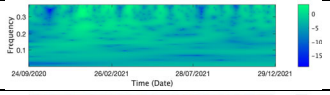
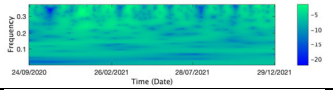
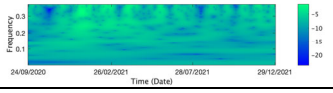
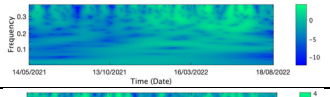
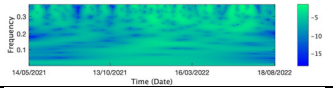
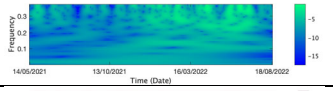
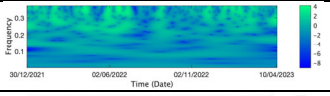
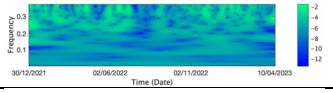
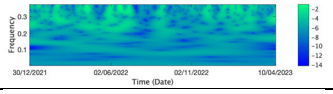
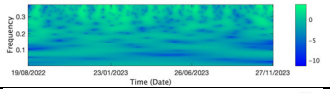
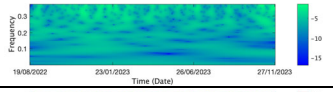
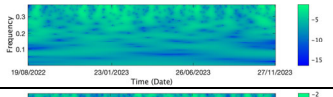
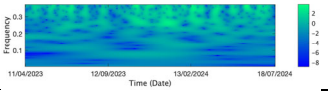
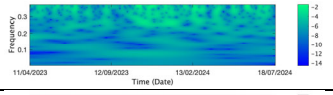
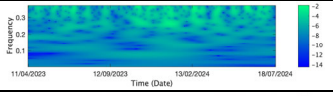
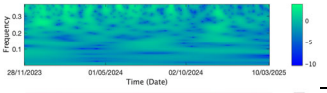
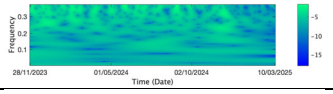
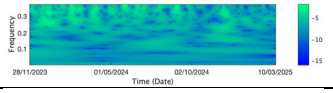
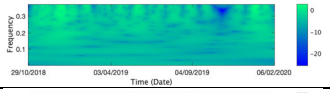
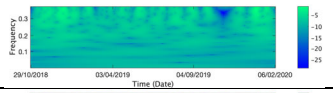
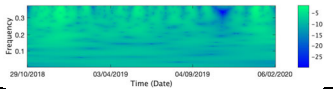
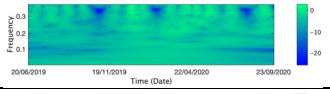
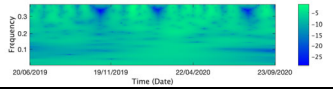
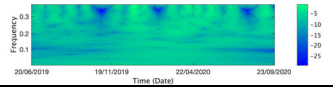
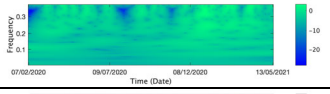
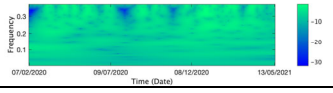
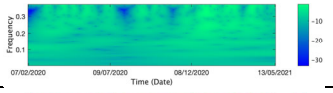
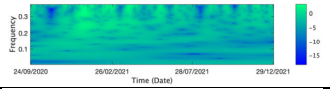
CI

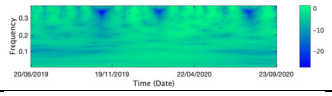
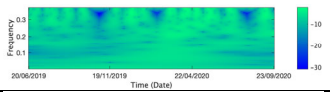
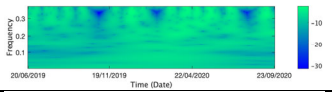
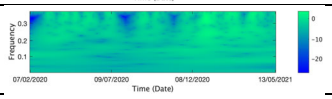
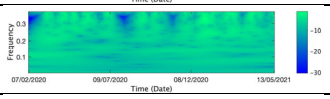
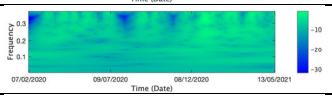
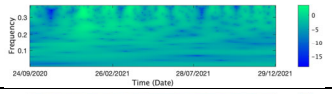
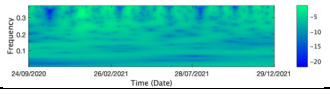
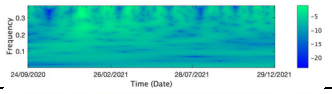
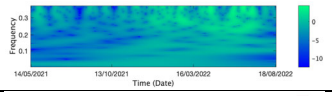
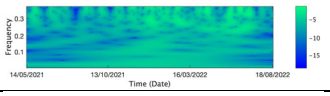
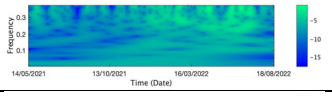
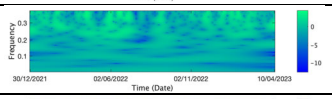
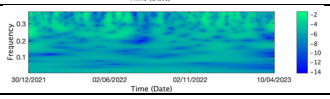
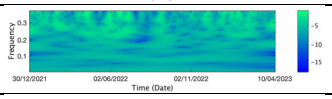
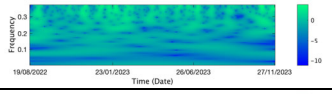
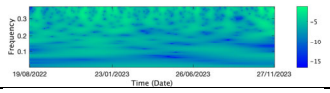
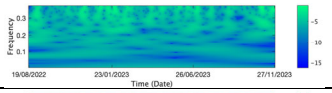
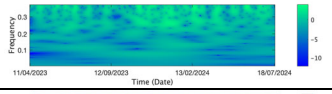
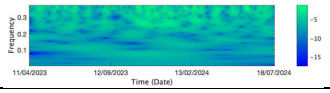
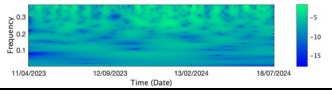
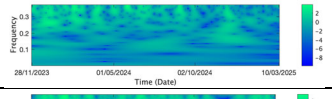
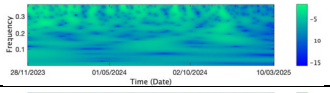
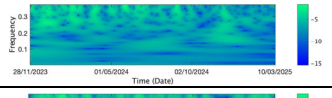
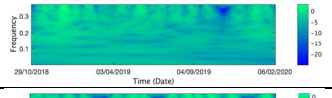
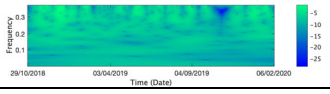
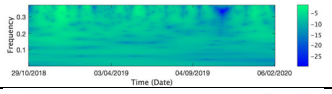
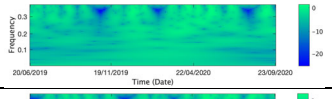
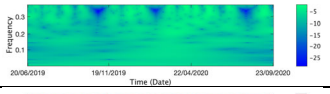
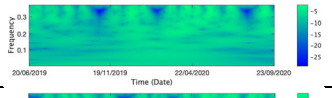
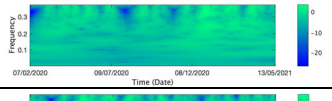
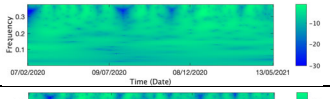
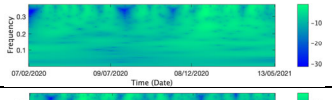
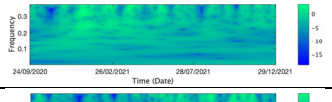
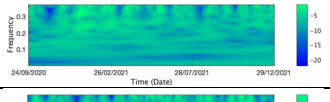
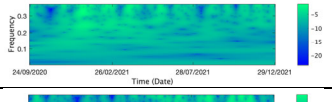
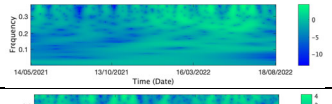
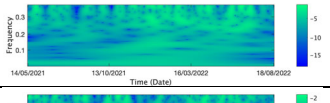
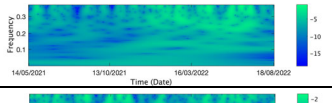
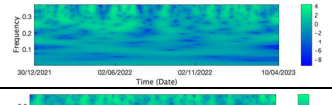
Note: The appendix summarizes the wavelet analysis results, showing the influence of cyberattacks, severity scores, and targeted critical infrastructure on clean energy indices across time windows. Colors indicate wavelet power, with cooler tones (light blue and cyan) showing lower power and warmer tones (green) indicating higher power. Arrows depict phase relationships: rightward for in-phase, leftward for antiphase, upward for first series leading, and downward for second series

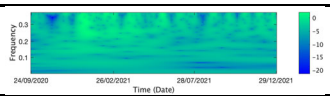
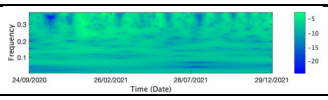
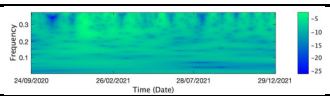
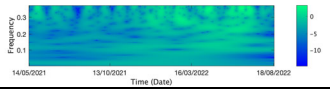
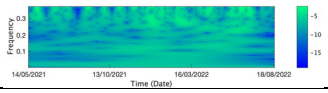
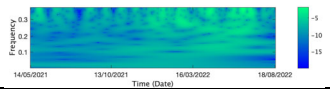
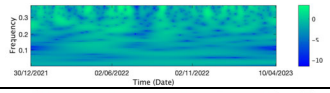
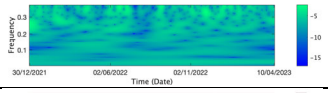
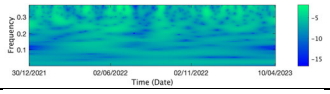
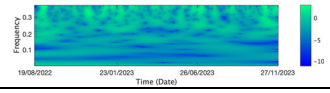
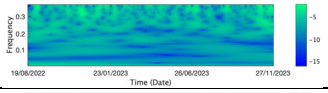
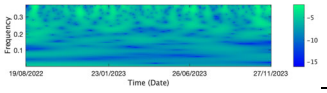
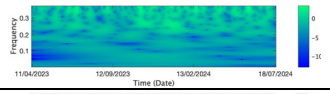
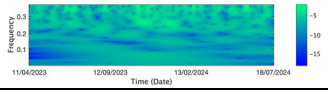
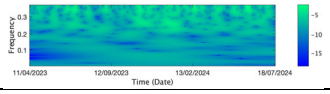
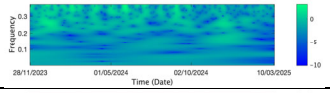
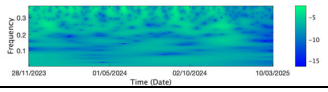
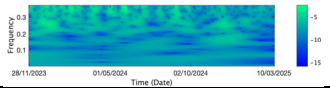
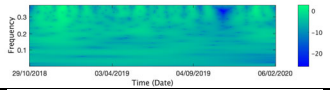
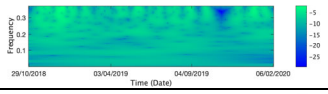
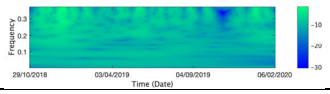
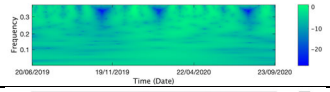
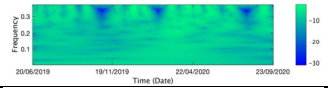
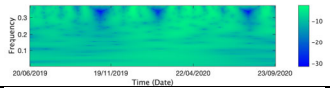
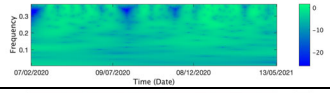
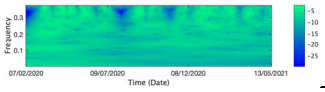
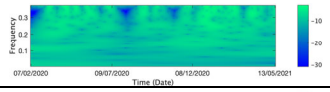
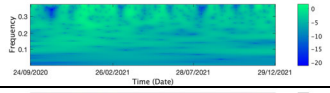
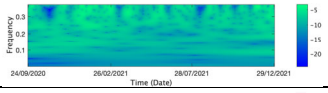
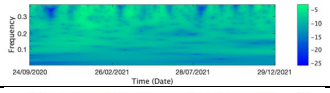
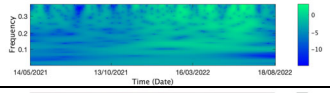
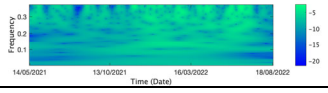
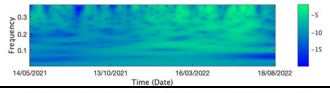
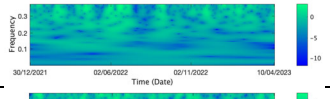
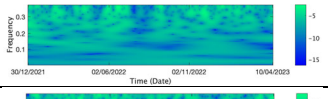
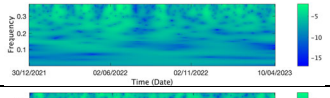
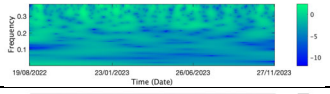
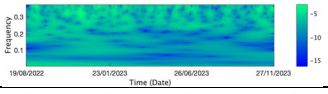
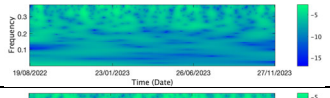
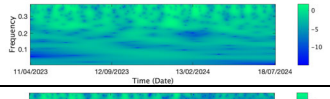
leading. The white cone represents the cone of influence, beyond which edge effects may distort the results.

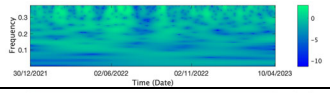
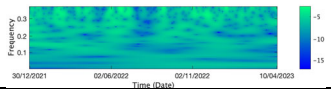
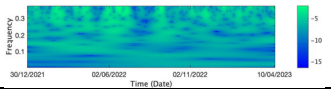
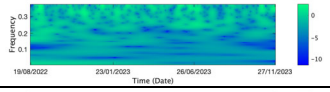
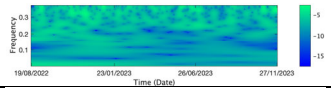
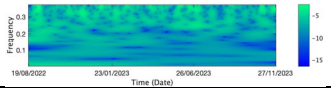
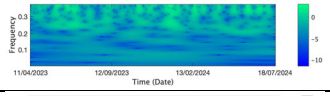
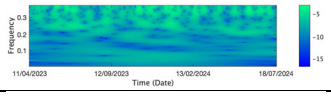
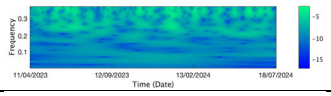
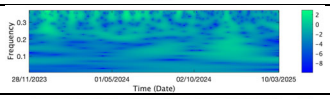
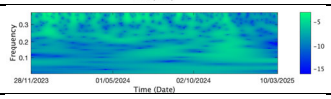
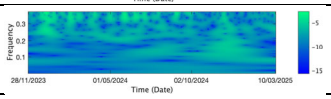
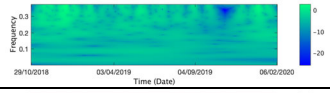
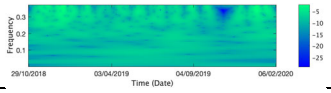
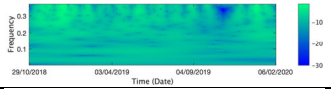
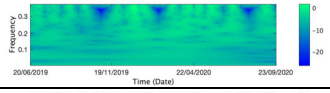
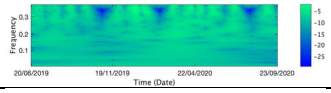
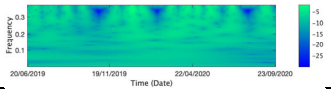
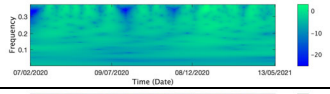
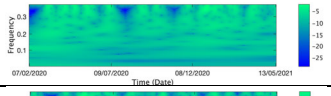
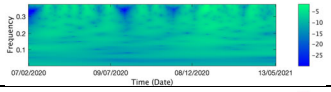
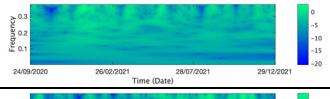
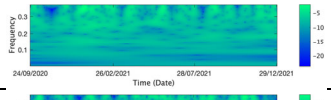
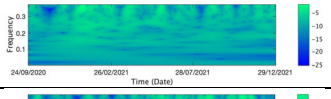
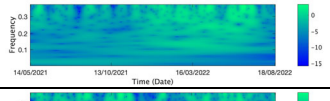
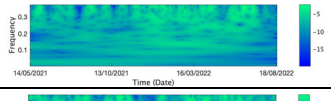
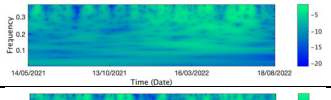
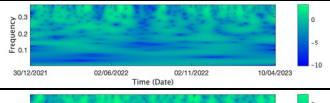
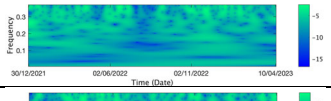
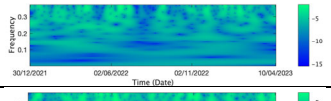
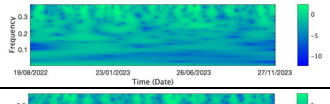
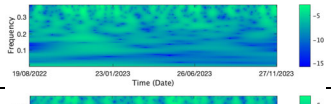
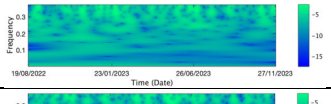
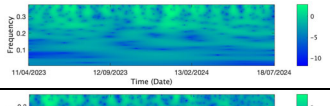
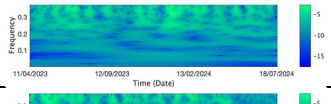
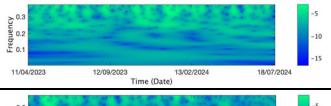
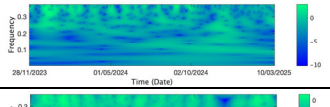
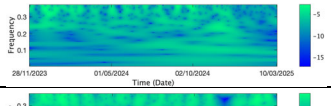
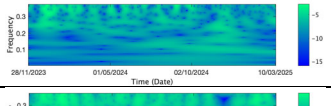
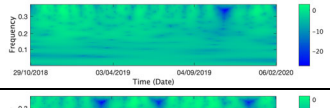
Appendix C. XWT Results

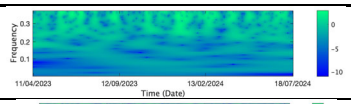
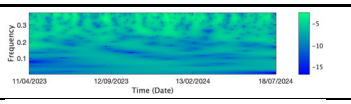
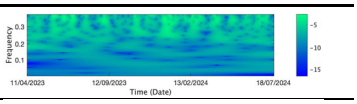
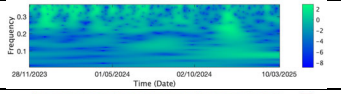
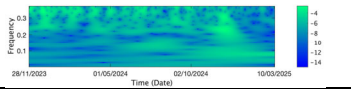
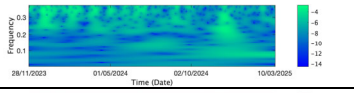
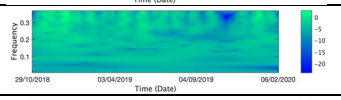
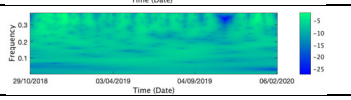
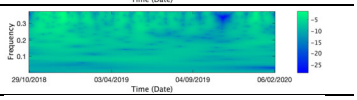
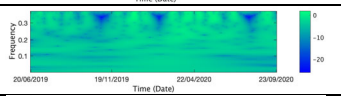
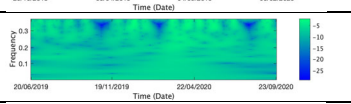
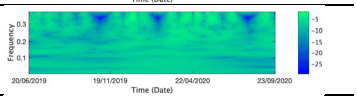
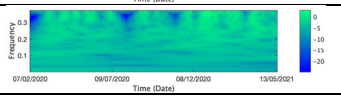
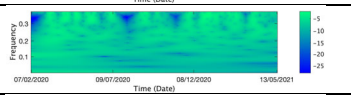
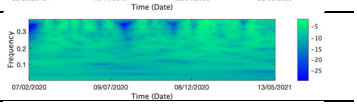
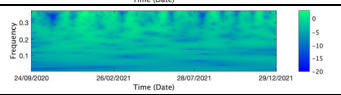
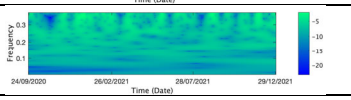
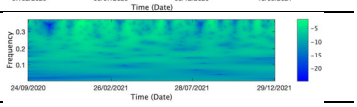
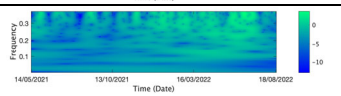
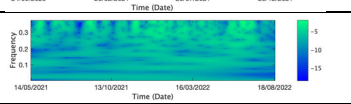
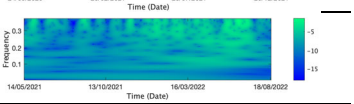
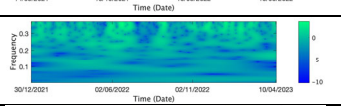
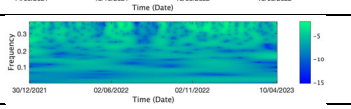
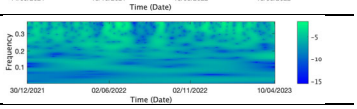
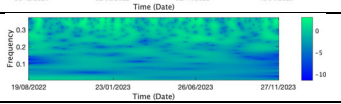
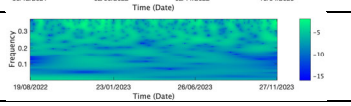
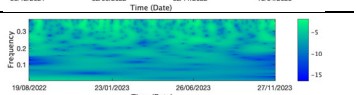
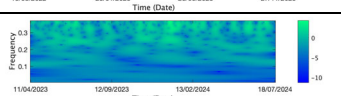
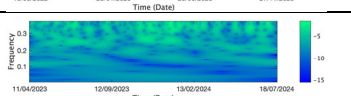
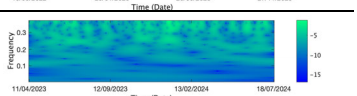
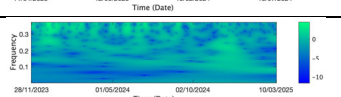
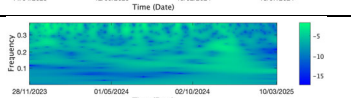
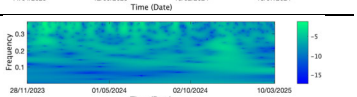
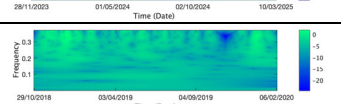
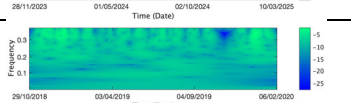
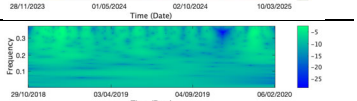
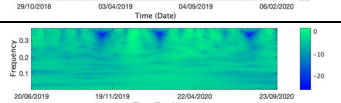
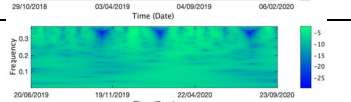
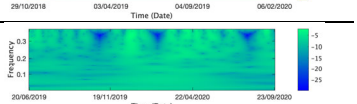
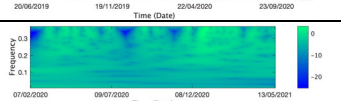
Index/ Window		CA	SS	CI
ICLN	1			
	2			
	3			
	4			
	5			
	6			
	7			
	8			
	9			
TAN	1			
	2			
	3			
	4			
	5			
	6			
	7			
	8			

	9			
QCLN	1			
	2			
	3			
	4			
	5			
	6			
	7			
	8			
	9			
CNRG	1			
	2			
	3			
	4			
	5			
	6			
	7			
	8			
	9			
ACES	1			

	2			
	3			
	4			
	5			
	6			
	7			
	8			
	9			
	1			
	2			
	3			
	4			
PBW	5			
	6			
	7			
	8			
	9			
	1			
RNRG	2			
	3			

	4			
	5			
	6			
	7			
	8			
	9			
	1			
	2			
	3			
	4			
ACWI	5			
	6			
	7			
	8			
	9			
	1			
	2			
IEUR	3			
	4			
	5			

	6			
	7			
	8			
	9			
	1			
	2			
	3			
	4			
EEMA	5			
	6			
	7			
	8			
	9			
	1			
	2			
	3			
EWZ	4			
	5			
	6			
	7			

	8			
	9			
EZA	1			
	2			
	3			
	4			
	5			
	6			
	7			
	8			
	9			
	1			
	2			
	3			
	4			
AFK	5			
	6			
	7			
	8			
	9			

Note: The appendix presents the interaction between cyberattacks, severity scores, and targeted critical infrastructure across different time windows. Colors represent the strength of the cross-wavelet spectrum, with cooler tones (light blue and cyan) indicating lower coherence and warmer tones (green) indicating higher coherence.

References

1. He, Z.; Khazaei, J.; Moazeni, F.; Freihaut, J.D. Detection of false data injection attacks leading to line congestions using neural networks. *Sustain. Cities Soc.* **2022**, *82*, 103861. https://doi.org/10.1016/j.scs.2022.103861.
2. Li, Y.; Ding, Y.; He, S.; Hu, F.; Duan, J.; Wen, G.; Geng, H.; Wu, Z.; Gooi, H.B.; Zhao, Y.; et al. Artificial intelligence-based methods for renewable power system operation. *Nat. Rev. Electr. Eng.* **2024**, *1*, 163–179. https://doi.org/10.1038/s44287-024-00018-9.
3. Vinuesa, R.; Azizpour, H.; Leite, I.; Balaam, M.; Dignum, V.; Domisch, S.; Felländer, A.; Langhans, S.D.; Tegmark, M.; Fuso Nerini, F. The role of artificial intelligence in achieving the Sustainable Development Goals. *Nat. Commun.* **2020**, *11*, 233. https://doi.org/10.1038/s41467-019-14108-y.
4. Tabansky, L.; Lichterman, E. Progress: The sectoral approach to cyber resilience. *Int. J. Inf. Secur.* **2025**, *24*, 18. https://doi.org/10.1007/s10207-024-00910-3.
5. Wang, L.; Wang, S. Unusual investor behavior under tacit and endogenous market signals. *Int. Rev. Econ. Financ.* **2021**, *73*, 76–97. https://doi.org/10.1016/j.iref.2020.12.029.
6. Eisenbach, T.M.; Kovner, A.; Lee, M.J. Cyber risk and the U.S. financial system: A pre-mortem analysis. *J. Financ. Econ.* **2022**, *145*, 802–826. https://doi.org/10.1016/j.jfineco.2021.10.007.
7. Elsayed, A.H.; Naifar, N.; Nasreen, S.; Tiwari, A.K. Dependence structure and dynamic connectedness between green bonds and financial markets: Fresh insights from time-frequency analysis before and during COVID-19 pandemic. *Energy Econ.* **2022**, *107*, 105842. https://doi.org/10.1016/j.eneco.2022.105842.
8. Ding, Q.; Huang, J.; Chen, J. Time-frequency spillovers and the determinants among fossil energy, clean energy and metal markets. *Energy J.* **2023**, *44*, 259–286. https://doi.org/10.5547/01956574.44.2.qdin.
9. Akyildirim, E.; Conlon, T.; Corbet, S.; Hou, Y. HACKED: Understanding the stock market response to cyberattacks. *J. Int. Financ. Mark. Inst. Money* **2024**, *97*, 102082. https://doi.org/10.1016/j.intfin.2024.102082.
10. Tosun, O.K. Cyber-attacks and stock market activity. *Int. Rev. Financ. Anal.* **2021**, *76*, 101795. https://doi.org/10.1016/j.irfa.2021.101795.
11. Cybersecurity and Infrastructure Security Agency (CISA). The Attack on Colonial Pipeline: What We've Learned and What We've Done over the Past Two Years. Available online: https://www.cisa.gov (accessed on 16 December 2024).
12. International Monetary Fund. Rising Cyber Threats Pose Serious Concerns for Financial Stability. Available online: https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability (accessed on 18 January 2025).
13. International Energy Agency. Annual Investment in Clean Energy by Selected Country and Region: 2019 and 2024. Available online: https://www.iea.org/data-and-statistics/charts/annual-investment-in-clean-energy-by-selected-country-and-region-2019-and-2024 (accessed on 11 January 2025).
14. Alkathery, M.A.; Chaudhuri, K.; Nasir, M.A. Dependence between the GCC energy equities, global clean energy and emission markets: Evidence from wavelet analysis. *Energy Econ.* **2023**, *121*, 106659. https://doi.org/10.1016/j.eneco.2023.106659.
15. Chen, T.; Yin, X.; Wang, G. Securing communications between smart grids and real users; providing a methodology based on user authentication. *Energy Rep.* **2021**, *7*, 8042–8050. https://doi.org/10.1016/j.egyr.2021.08.125.
16. Chatziantoniou, I.; Abakah, E.J.A.; Gabauer, D.; Tiwari, A.K. Quantile time–frequency price connectedness between green bond, green equity, sustainable investments and clean energy markets. *J. Clean. Prod.* **2022**, *361*, 132088. https://doi.org/10.1016/j.jclepro.2022.132088.
17. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 107094. https://doi.org/10.1016/j.comnet.2019.107094.
18. Markowitz, H. Portfolio selection. *J. Financ.* **1952**, *7*, 77–91. https://doi.org/10.2307/2975974.
19. Spence, M. Job market signaling. *Q. J. Econ.* **1973**, *87*, 355–374. https://doi.org/10.2307/1882010.
20. Fama, E.F. Efficient capital markets: A review of theory and empirical work. *J. Financ.* **1970**, *25*, 383–417. https://doi.org/10.2307/2325486.
21. Federal Energy Regulatory Commission (FERC). Solar Winds and Related Supply Chain Compromise [White Paper]. Available online: https://www.ferc.gov (accessed on 15 December 2024).
22. OWASP. OWASP Risk Rating Methodology. Available online: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology (accessed on 13 December 2024).
23. Arfaoui, N.; Naeem, M.A.; Boubaker, S.; Mirza, N.; Karim, S. Interdependence of clean energy and green markets with cryptocurrencies. *Energy Econ.* **2023**, *120*, 106584. https://doi.org/10.1016/j.eneco.2023.106584.
24. El-Afifi, M.I.; Sedhom, B.E.; Padmanaban, S.; Eladl, A.A. A review of IoT-enabled smart energy hub systems: Rising, applications, challenges, and future prospects. *Renew. Energy Focus* **2024**, *51*, 100634. https://doi.org/10.1016/j.ref.2024.100634.
25. Venkatesan, K.; Rahayu, S.B. Blockchain security enhancement: An approach towards hybrid consensus algorithms and machine learning techniques. *Sci. Rep.* **2024**, *14*, 1149. https://doi.org/10.1038/s41598-024-51578-7.

26. Qin, M.; Zhang, X.; Li, Y.; Badarcea, R.M. Blockchain market and green finance: The enablers of carbon neutrality in China. *Energy Econ.* **2023**, *118*, 106501. https://doi.org/10.1016/j.eneco.2022.106501.
27. Lawal, O.A.; Teh, J.; Alharbi, B.; Lai, C.-M. Data-driven learning-based classification model for mitigating false data injection attacks on dynamic line rating systems. *Sustain. Energy Grids Netw.* **2024**, *38*, 101347. https://doi.org/10.1016/j.segan.2024.101347.
28. Mitra, S.; Chakraborty, B.; Mitra, P. Smart meter data analytics applications for secure, reliable and robust grid system: Survey and future directions. *Energy* **2024**, *289*, 129920. https://doi.org/10.1016/j.energy.2023.129920.
29. Hu, Q.; Bu, S.Q.; Su, W.; Terzija, V. A privacy-preserving energy management system based on homomorphic cryptosystem for IoT-enabled active distribution network. *J. Mod. Power Syst. Clean Energy* **2024**, *12*, 167–178. https://doi.org/10.35833/MPCE.2022.000507.
30. Mishra, D.K.; Wang, J.; Li, L.; Zhang, J.; Hossain, M.J. Resilience-driven scheme in multiple microgrids with secure transactive energy system framework. *IEEE Trans. Ind. Appl.* **2024**, *60*, 2277–2289. https://doi.org/10.1109/TIA.2023.3299260.
31. Lucey, B.; Ren, B. Time-varying tail risk connectedness among sustainability-related products and fossil energy investments. *Energy Econ.* **2023**, *126*, 106812. https://doi.org/10.1016/j.eneco.2023.106812.
32. Tiwari, A.K.; Kumar, S.; Abakah, E.J.A. Correlation and price spillover effects among green assets. *Ann. Oper. Res.* **2024**, 1–26. https://doi.org/10.1007/s10479-024-06154-7.
33. Boakye, D.; Sarpong, D.; Meissner, D.; Ofosu, G. How TalkTalk did the walk-walk: Strategic reputational repair in a cyber-attack. *Inf. Technol. People* **2024**, *37*, 1642–1673. https://doi.org/10.1108/ITP-08-2022-0589.
34. Husain, S.; Sohag, K.; Wu, Y.R. The responsiveness of renewable energy production to geopolitical risks, oil market instability and economic policy uncertainty: Evidence from United States. *J. Environ. Manag.* **2024**, *350*, 119647. https://doi.org/10.1016/j.jenvman.2023.119647.
35. Demiralay, S.; Gencer, H.G.; Bayraci, S. Carbon credit futures as an emerging asset: Hedging, diversification and downside risks. *Energy Econ.* **2022**, *113*, 106196. https://doi.org/10.1016/j.eneco.2022.106196.
36. Yousaf, I.; Mensi, W.; Vo, X.V.; Kang, S.H. Dynamic spillovers and connectedness between crude oil and green bond markets. *Resour. Policy* **2024**, *89*, 104594. https://doi.org/10.1016/j.resourpol.2023.104594.
37. Investing.com. Official Website. Available online: https://www.investing.com/ (accessed on 11 January 2025).
38. Yahoo Finance. Official Website. Available online: https://finance.yahoo.com (accessed on 11 January 2025).
39. Bloomberg Terminal. Official Website. Available online: https://www.bloomberg.com (accessed on 12 January 2025).
40. Privacy Rights Clearinghouse. Official Website. Available online: https://privacyrights.org (accessed on 14 January 2025).
41. Hackmageddon. Official Website. Available online: https://www.hackmageddon.com (accessed on 15 January 2025).
42. Eurepoc. Official Website. Available online: https://eurepoc.eu (accessed on 15 January 2025).
43. Center for Strategic and International Studies (CSIS). Official Website. Available online: https://www.csis.org (accessed on 16 January 2025).
44. Koop, G.; Korobilis, D. A new index of financial conditions. *Eur. Econ. Rev.* **2014**, *71*, 101–116. https://doi.org/10.1016/j.euroecorev.2014.07.002.
45. Gabauer, D.; Gupta, R. On the transmission mechanism of country-specific and international economic uncertainty spillovers: Evidence from a TVP-VAR connectedness decomposition approach. *Econ. Lett.* **2018**, *171*, 63–71. https://doi.org/10.1016/j.econlet.2018.07.007.
46. Erenoğlu, A.K.; Sengor, I.; Erdinç, O. Power system resiliency: A comprehensive overview from implementation aspects and innovative concepts. *Energy Nexus* **2024**, *15*, 100311. https://doi.org/10.1016/j.nexus.2024.100311.
47. Song, Y.; Bouri, E.; Ghosh, S.; Kanjilal, K. Rare earth and financial markets: Dynamics of return and volatility connectedness around the COVID-19 outbreak. *Resour. Policy* **2021**, *74*, 102379. https://doi.org/10.1016/j.resourpol.2021.102379.
48. Alomari, M.; Khoury, R.E.; Mensi, W.; Vo, X.V.; Kang, S.H. Extreme downside risk connectedness between green energy and stock markets. *Energy* **2024**, *312*, 133477. https://doi.org/10.1016/j.energy.2024.133477.
49. Urom, C.; Ndubuisi, G.; Mzoughi, H.; Guesmi, K. Exploring the coherency and predictability between the stocks of artificial intelligence and energy corporations. *Financ. Innov.* **2024**, *10*, 128. https://doi.org/10.1186/s40854-024-00609-3.
50. Antonakakis, N.; Chatziantoniou, I.; Gabauer, D. Refined measures of dynamic connectedness based on time-varying parameter vector autoregressions. *J. Risk Financ. Manag.* **2020**, *13*, 84. https://doi.org/10.3390/jrfm13040084.
51. Doğan, B.; Ben Jabeur, S.; Tiwari, A.K.; Abakah, E.J.A. Asymmetry in returns and volatility between green financial assets, sustainable investments, clean energy, and international stock markets. *Res. Int. Bus. Financ.* **2025**, *73*, 101212. https://doi.org/10.1016/j.ribaf.2024.102626.
52. Vargas, P.; Tien, I. Impacts of 5G on cyber-physical risks for interdependent connected smart critical infrastructure systems. *Int. J. Crit. Infrastruct. Prot.* **2023**, *42*, 100617. https://doi.org/10.1016/j.ijcip.2023.100617.
53. Pettersen, S.; Grøtan, T.O. Exploring the grounds for cyber resilience in the hyper-connected oil and gas industry. *Saf. Sci.* **2024**, *171*, 106384. https://doi.org/10.1016/j.ssci.2023.106384.
54. Sallos, M.-P.; Garcia Perez, A.; Bocanet, A. Organisational cyber resilience: A heuristic for bridging foundations and applications. *J. Enterp. Inf. Manag.* **2024**, *37*, 1926–1952. https://doi.org/10.1108/JEIM-06-2023-0317.
55. Ziadat, S.A.; Mensi, W.; Al-Kharusi, S.H.; Vo, X.V.; Kang, S.H. Are clean energy markets hedges for stock markets? A tail quantile connectedness regression. *Energy Econ.* **2024**, *136*, 106286. https://doi.org/10.1016/j.eneco.2024.107757.
56. Gabriel, V.; Pinho, C. Are clean and black energy exchange-traded funds driven by climate risk? *J. Sustain. Financ. Invest.* **2024**, 1–27. https://doi.org/10.1080/20430795.2024.2303501.

57. Bloomberg NEF. Global Clean Energy Investment Jumps 17%, Hits $1.8 Trillion in 2023. Available online: https://about.bnef.com/blog/global-clean-energy-investment-jumps-17-hits-1-8-trillion-in-2023-according-to-bloombergnef-report (accessed on 11 January 2025).
58. Yao, C.Z.; Mo, Y.N.; Zhang, Z.K. A study of the efficiency of the Chinese clean energy stock market and its correlation with the crude oil market based on an asymmetric multifractal scaling behavior analysis. *N. Am. J. Econ. Financ.* **2021**, *58*, 101520. https://doi.org/10.1016/j.najef.2021.101520.
59. Arcuri, M.C.; Gai, L.; Ielasi, F.; Ventisette, E. Cyber attacks on hospitality sector: Stock market reaction. *J. Hosp. Tour. Technol.* **2020**, *11*, 277–290. https://doi.org/10.1108/JHTT-05-2019-0080.
60. Xiao, X.Y.; Li, A.X.; Kchouri, B.; Shan, S. Tracing the dynamic impact of energy transitions on equity market volatility in an era of financial turbulence. *Energy Econ.* **2024**, *133*, 106652. https://doi.org/10.1016/j.eneco.2024.107443.
61. Lee, I. Cybersecurity: Risk management framework and investment cost analysis. *Bus. Horiz.* **2021**, *64*, 659–671. https://doi.org/10.1016/j.bushor.2021.02.022.
62. Halgamuge, M.N. Leveraging deep learning to strengthen the cyber-resilience of renewable energy supply chains: A survey. *IEEE Commun. Surv. Tutor.* **2024**, *26*, 2146–2175. https://doi.org/10.1109/COMST.2024.3365076.
63. Wu, R.R.; Liu, B.Y. Do climate policy uncertainty and investor sentiment drive the dynamic spillovers among green finance markets? *J. Environ. Manag.* **2023**, *347*, 119008. https://doi.org/10.1016/j.jenvman.2023.119008.
64. Sharma, G.D.; Shahbaz, M.; Singh, S.; Chopra, R.; Cifuentes-Faura, J. Investigating the nexus between green economy, sustainability, bitcoin and oil prices: Contextual evidence from the United States. *Resour. Policy* **2023**, *80*, 103168. https://doi.org/10.1016/j.resourpol.2022.103168.
65. Yadav, M.P.; Ashok, S.; Taghizadeh-Hesary, F.; Dhingra, D.; Mishra, N.; Malhotra, N. Uncovering time and frequency co-movement among green bonds, energy commodities and stock market. *Stud. Econ. Financ.* **2024**, *41*, 638–659. https://doi.org/10.1108/SEF-03-2023-0126.
66. Thi Xuan, H.; Thai Hung, N. Does green investment mitigate environmental degradation in Vietnam: The time-frequency effect of nonrenewable energy investment and globalization? *Manag. Environ. Qual.* **2024**, *35*, 1005–1027. https://doi.org/10.1108/MEQ-09-2023-0332.
67. Zhang, L.; Wang, L.; Nguyen, T.T.; Ren, R. Volatility forecasting of clean energy ETF using GARCH-MIDAS with neural network model. *Financ. Res. Lett.* **2024**, *70*, 106286. https://doi.org/10.1016/j.frl.2024.106286.
68. Abakah, E.J.A.; Wali Ullah, G.; Adekoya, O.B.; Osei Bonsu, C.; Abdullah, M. Blockchain market and eco-friendly financial assets: Dynamic price correlation, connectedness and spillovers with portfolio implications. *Int. Rev. Econ. Financ.* **2023**, *87*, 218–243. https://doi.org/10.1016/j.iref.2023.04.028.
69. Osman, R.; El-Gendy, S. Interconnected and resilient: A CGE analysis of AI-driven cyberattacks in global trade. *Risk Anal.* **2024**, 1–17. https://doi.org/10.1111/risa.14321.
70. Farrand, B. The economy–security nexus: Risk, strategic autonomy and the regulation of the semiconductor supply chain. *Eur. J. Risk Regul.* **2024**, 1–15. https://doi.org/10.1017/err.2024.63.