Journal of Business Insight and Innovation

Volume 4 Issue 2, 2025
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

BUSINESS INTELLIGENCE AS A STRATEGIC ASSET: MEASURING ITS ROLE IN ENHANCING U.S. NATIONAL INTERESTS ACROSS DEFENSE, TRADE, AND CYBER DOMAINS

Yeasin Arafat [1]

Affiliations:

[1] Information Technology Services, Administration, and Management,
St. Francis College, NY, USA

Email:
yeasinarafat1800@gmail.com

Corresponding Author(s) Email:

[1] yeasinarafat1800@gmail.com

Abstract

Business Intelligence (BI) has become an essential part of national strategic infrastructure in the face of escalating geopolitical volatility, surging cyber threats and disruption to the economy. This paper examines how BI is a strategic resource that can help United States in promoting national interests in three interconnected spheres: cybersecurity, defense, and trade. With empirical data based on the findings of professionals in these areas, the study discovers considerable correlations between BI use and strategic performance. Deployment of BI was a significant indicator of the strategic asset perception (beta = 0.33, R 2 = 0.28, p < 0.0001), whereas situational awareness of the defense (OR = 2.86, p = 0.007) and perceived cyber adequacy (OR = 2.08, p = 0.019) were also proven to play significant roles in strategic valuation. ANOVA and correlational tests also support the relevance of BI whereby the statistically significant relationship between familiarity with BI and cyber readiness (F = 3.18, p = 0.017) was obtained and the relationship between trade strategy shaping and cyber adequacy (r = 0.34, p = 0.0002) was discovered. As the technical integration of BI systems increases, evidence shows that there remains a difference between the operationalization and the strategic perception. The study concludes that in order to maximize the potential of BI in protection of national interests, institutional structures should focus on strategic integration, cross-sectorial policy consistency, and leadership-based BI literacy programs.

Keywords: Business Intelligence, Strategic Asset, U.S. National Security, Cyber Readiness, Defense Intelligence, Trade Strategy, Data-Driven Governance

Introduction

In the age of geopolitical rivalry and digital revolution, the information has turned into one of the most effective strategic assets. Business Intelligence (BI) that began in the context of corporate decision-making and performance optimization is starting to become a national infrastructure that enables national security, resilience of the economy and cyber defense. The rising sophistication of threats around the world such as state-sponsored cyber-attacks, economic shocks, among others have highlighted the importance of using data not only in operational but also strategic ways. In the case of the United States, it is not the availability of data that is a problem but actually leveraging that data in real-time to make a decision and it is in this realm that BI is revolutionary. BI involves systems, technologies, and methods of collecting, analyzing, and presentation of data to aid in decision-making. It has advanced quite a bit, with the ability to provide real-time dashboards, predictive analytics, and anomaly detection in large, heterogeneous streams of data. Such abilities are especially important in the overlapping needs of cybersecurity, defense preparedness, and trade competitiveness. BI has emerged as a strategic force multiplier and it has been adopted by the United States

Journal of Business Insight and Innovation

Volume 4 Issue 2, 2025
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

agencies and organizations in recent years to address these demands (Basharat et al., 2025; Ogborigbo et al, 2024).

The US is confronted with a new level and magnitude of cyber-attacks, some of which are initiated by state-sponsored entities that attack critical infrastructure, financial infrastructures, and military networks. BI systems (combined with threat intelligence platforms) increase the identification of suspicious activity, enhance situational awareness and aid in making decisions as soon as possible (Qayyum et al., 2025; Sun et al, 2023). AlDaajeh et al. (2022) highlight that BI tools, national cybersecurity strategies are well aligned, and such a combination is likely to enhance readiness and response capacities, particularly with the help of a trained workforce and institutionalization. The military has also discovered the tactical value of BI. Lemieux (2024) argues that the application of BI to intelligence collection and defense initiatives enables more flexible, data-driven decision-making, which is an essential condition of military interaction in the modern environment. With strategic stability being threatened by the application of artificial intelligence and cyber capabilities in the hands of adversaries, the United States has to make sure that its defense systems are backed up by equally developed BI infrastructures (Ahmad & Museera, 2024; Hunter et al, 2024).

Besides defense and cyber, BI is also influential in defining how the U.S. pursues economic and trade policies. Disruption of the global supply chain, barriers to trade in the digital space and uncertainty of regulation have necessitated the need to have dynamic policy planning based on data. Han (2024) states that data localization and economic nationalism are not peripheral issues but central to national strategy anymore. This study aims to take a critical look at whether Business Intelligence is a strategic tool or asset in the strengthening of national interests of the United States in three inseparable spheres, namely, defense, cybersecurity and trade. This study will help to fill the gap between conceptual knowledge and empirical experience to illustrate the strategic importance of BI in the protection of U.S. sovereignty, anticipatory governance, and cross-sector resilience in the context of an increasingly complex global environment.

Literature Review

Business Intelligence as a Strategic Asset

Business Intelligence (BI) has transformed to become more of a strategic enabler in both the public and the private sectors since it started as a performance management tool. Traditionally linked to efficiency in an organization, BI has evolved and currently includes predictive analytics, real-time data visualization and decision support systems (Butt & Shah, 2025; Ogborigbo et al., 2024). Such capabilities make BI a major tool in dealing with uncertainty, foresight and institutional and national resilience.

Several researchers have highlighted the new role of BI in the governance of a country. Lemieux (2024) points to the fact that BI platforms are becoming an element of intelligence operations to enhance surveillance, threat forecasting and resource management. Equally, Weaver (2022) recognizes analytical bottlenecks in U.S. cybersecurity and intelligence systems that can be resolved by enhancing BI integration. The greater transition in reactive to proactive information strategies highlights the significance of BI as a tool of operations as well as national preparedness infrastructure.

BI and Cybersecurity Strategy

Cybersecurity has emerged as a fundamental national security problem and cyber-attacks have focused more on the systems of governments, defense infrastructure, and critical infrastructure. BI systems are the key element in this environment as they improve the detection of cyber threats, incident response and tracking anomalies (Sun et al, 2023). In support of this argument, AlDaajeh et al. (2022) believe that BI should be incorporated into national cybersecurity initiatives to encourage the idea of constant monitoring, machine analysis and agile defense stances.

The association between BI and cybersecurity is further entrenched by the emergence of cyber tools powered with AI (Butt, 2021). Due to the use of generative AI to create disinformation and malware by adversaries, the intelligence-enabled defense has become increasingly relevant (Hunter et al, 2024; Sadia, 2020). Dhoni & Kumar (2023) discussed the composition of AI and BI in terms of their synergistic capabilities in identifying advanced persistent threats and constructing cyber risk scenarios. Verma et al. (2025) also

Journal of Business Insight and Innovation
Volume 4 Issue 2, 2025
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

emphasize that cyber resilience strategies need to be operationalized through the use of BI systems in such industries as the finance and energy sectors, where it is crucial to respond to the incidents within a short period of time.

BI in Defense and Intelligence Operations

BI is being used more and more in defense in operational awareness, forecasting logistics, and strategy planning. Since the nature of war is moving into the digital and cognitive arenas, information dominance becomes one of the primary goals (Sharpe et al, 2025). BI solutions are used to integrate battlefield information, evaluate threat vectors and resource allocation in real-time by military establishments.

Zegart et al. (2023) present a different conceptualization of a cyber-conflict, namely, as an intelligence contest, a contest between countries on not only the level of armaments but also the level of quickness and quality of decision-making. BI improves command-and-control operations in this setting, by lowering the time delay of analyses and clarity in uncertainty. According to McGeachy (2022), strategic infrastructure, which includes submarine cables, satellite systems, etc., is becoming more dependent on BI-driven surveillance systems to facilitate continuity and security. The authors also examine the role BI-powered cybersecurity is playing in the defense policy in new areas such as outer space, where the nature of the threat environment requires real-time analytics and cross-domain planning and coordination (Cappelletti & Papakonstantinou, 2025; Butt & Yazdani, 2023).

BI and Trade Policy Intelligence

The rise in economic security as a cornerstone of national security has seen BI used more and more to aid trade negotiations, to help track market volatility and to evaluate geopolitical risk. Broeders et al. (2023) emphasize the protection of digital sovereignty and strategic autonomy in the arena of trade through the BI. Trade ministries and financial regulators to track global supply chains, find fraud and trial policy impacts now use BI platforms. Han (2024) also argues about data localization policies as an economic statecraft tool, noting that countries such as the U.S. should invest in the domestic BI capacity to ensure their competitiveness. As demonstrated by Paul et al. (2023) and Ekechukwu & Simpa (2024), BI-based monitoring systems are currently employed to track financial malpractices and safeguard foreign investment, particularly in the sectors exposed to cyber-attacks or regulatory manipulation.

Strategic foresight is also enhanced by incorporation of BI in trade. BI systems, according to Radanliev (2025), enable countries to react to the changes in economic and regulatory environments more quickly, thereby mitigating the risk of exposure to asymmetric economic threats.

Identified Gaps and Study Rationale

Although previous research confirms the vital importance of BI in cyber, defense and trade industries, some restrictions are present. First, the majority of the studies analyze BI on an organizational or sectorial level, not national. Second, although the technical advantages of BI have been reported upon, less empirical attention has been given to the manner in which BI is perceived, integrated, and strategically aligned within U.S. institutions. Third, available literature does not focus on the intersection of cybersecurity, defense, and trade concurrently, although the three are becoming intertwined in reality.

This research addresses the above gaps through examining the perceived strategic value of BI in various sectors in the United States and with a national perspective. It examines the connection between the use of BI and its applications to the national interests and provides a multi-level perspective on how data systems are redefining 21st century strategy.

Methodology

Research Design

The research was based on the quantitative, cross-sectional survey that was used to evaluate the perception and strategic positioning of Business Intelligence (BI) in the spheres of cybersecurity, defense, and trade in the United States. This design enabled to collect standardized information on a heterogeneous sample of professionals operating in national interest fields, permitting comparative analysis and statistically based understandings of the position of BI as a strategic resource.

Journal of Business Insight and Innovation

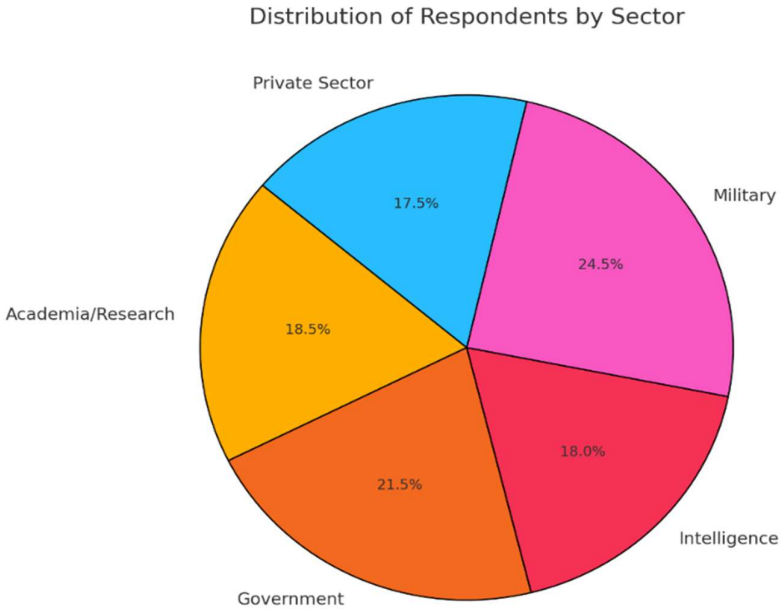
Volume 4 Issue 2, 2025
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Participants and Sampling

There were 200 participants in the study and the respondents were selected in five large areas: military, government, private industry, academia/research and the intelligence community. To facilitate the inclusion of all respondents, the study employed a purposive sampling method so that all the respondents had pertinent knowledge or decision-making skills in the area of national security, cyber policy, or economic strategy. The demographic profile of participants included data regarding the level of education, working experience and current area, which made it possible to compare subgroups and analyze the situation.

Figure 1

Distribution of Respondents by Sector



Research Instrument and Data Analysis

A structured and close-ended questionnaire was the main tool of data collection, divided into five parts: (1) the demographic characteristics, (2) familiarity and use of BI, (3) the perception of the strategic value of BI, (4) the relevance of BI to the sector-specific fields (cybersecurity, defense, and trade), (5) the organizational alignment, and integration of BI. The questions were put in Likert-scale format in order to quantify attitudes and perceptions. A small sample of domain professionals was used to pilot-test the survey instrument in order to clarify the wording of questions and increase the internal consistency of the instrument before implementing it.

The survey was sent over the social platforms through professional networks such as LinkedIn, company mailing lists and industry-specific forums that involve cybersecurity, defense, and economic policy experts. The data collection was kept open during a period of four weeks to ensure proper build-up of responses and at the same time keep the data relevant. They were told about the academic character of the study, promised to remain anonymous and had a right to withdraw.

The statistical data analysis was carried out through SPSS statistical software. The description of the characteristics of the respondents and overall trends in the familiarity and perceptions of BI were initially described through descriptive statistics. A number of inferential statistical methods were used to test relationships among variables. The use of chi-square tests was to test the relationship between categorical variables like a sector affiliation and BI usage. The Pearson and Spearman correlation coefficients were used to determine the direction and strength of a linear and ordinal relationship. ANOVA and Kruskal Wallis tests were used to compare groups in terms of sector, education level, and BI exposure. The binary logistic

Journal of Business Insight and Innovation
Volume 4 Issue 2, 2025
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

regression, as well as linear regression, were used to evaluate predictors of strategic BI perception. Each test had a p-value of 0.05 or less and effect sizes were further represented as the basis of interpretation depth.

Ethical Considerations

The study adhered to all the pertinent ethics of conducting research among human subjects. Electronic informed consent was used and all answers were anonymous. Personal identifiers were not collected and data were stored in a secure place. It was purely voluntary and the withdrawal without any penalty was mentioned clearly.

Results

Demographic and Professional Profile of Respondents

The results of the distribution of the 200 respondents into the professional sectors and years of experience are provided in Table 1. The sample is balanced in major areas of institutional considerations to the focus of the research. The greatest percentage of respondents represented military (24.5%) and government (21.5%) and academic or research institutions (18.5%) sectors. Notably, almost a fifth of respondents were part of the intelligence community (18.0%), which emphasizes the strategic importance of their input on the national security topics. The commercial and technological dimension of BI applications also came in a significant contribution of 17.5% of the sample size in the private sector. The participants had relatively advanced professional experience with 33.0% reporting to have more than 20 years and another 22.5% having 11-20 years. This indicates that more than half of the respondents (55.5%) had more than ten years of hands-on experience, which strengthens the validity and maturity of their strategic analysis of Business Intelligence systems.

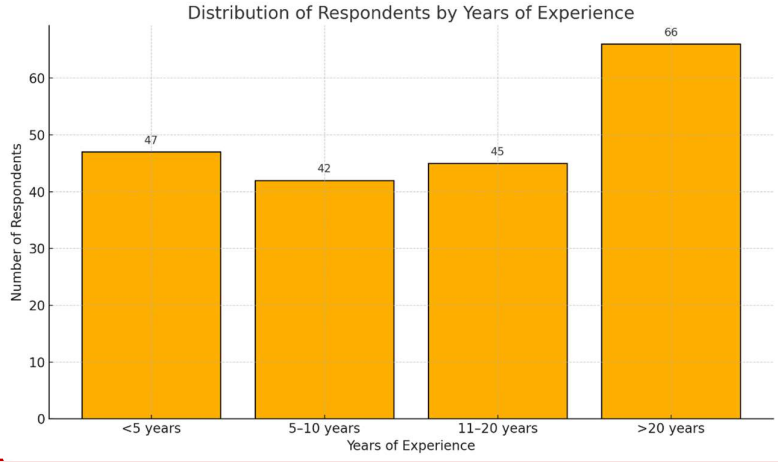
Table 1

Respondent Background by Sector and Experience (N = 200)

Variable	Category	Frequency	Percent (%)
Sector	Academia or Research Institution	37	18.5
	Government	43	21.5
	Intelligence Community	36	18.0
	Military	49	24.5
	Private Sector	35	17.5
Experience	Less than 5 years	47	23.5
	5–10 years	42	21.0
	11–20 years	45	22.5
	More than 20 years	66	33.0

Figure 2

Distribution of Respondents by Years of Experience



Journal of Business Insight and Innovation

Volume 4 Issue 2, 2025
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Educational Background and Familiarity with Business Intelligence

The education qualification of the respondents (Table 2) demonstrates that they are well prepared academically and professionally. More than half (56.5%) had graduate-level degrees, either a Master Degree (28.5%) or a Doctoral Degree (20.5%) and 28.0% had professional certification, which frequently signifies technical skills. This scholarly background explains why their observations of complex BI systems are credible.

Regarding the Business Intelligence familiarity, the findings showed a bias in the direction of a greater exposure. 45% were persons of the expert's level (23.5%) or very familiar (21.5%) with BI tools and applications.

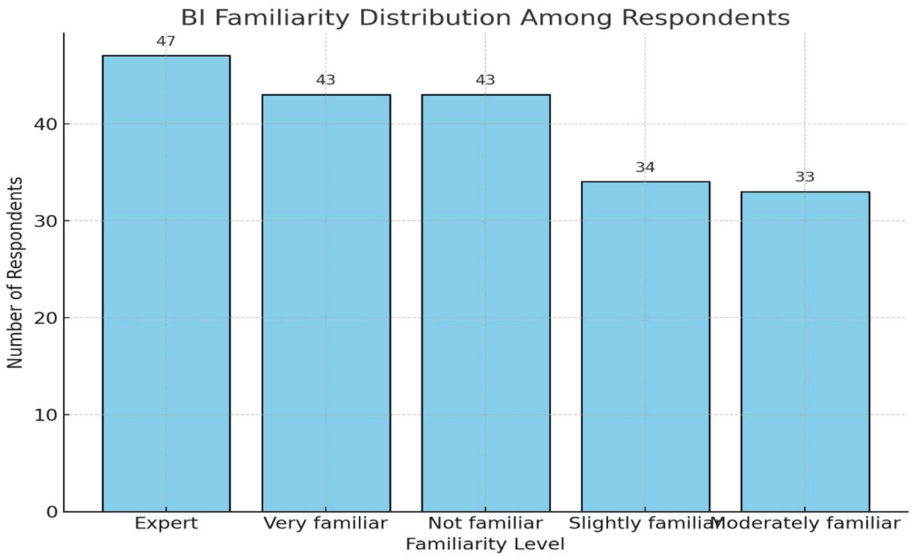
Table 2

Respondent Education and BI Familiarity (N = 200)

Variable	Category	Frequency	Percent (%)
Education	Bachelor's Degree	46	23.0
	Master's Degree	57	28.5
	Doctoral Degree	41	20.5
	Professional Certification	56	28.0
BI Familiarity	Expert level	47	23.5
	Very familiar	43	21.5
	Not familiar	43	21.5
	Slightly familiar	34	17.0
	Moderately familiar	33	16.5

Figure 3

BI Familiarity Distribution among Respondents



Chi-Square Analysis of Strategic BI Perceptions

Table 3 shows the outcomes of chi-square tests done to test the associations between perceptions of Business Intelligence (BI) and its strategic roles. Although the majority of the tested relationships were not found to be statistically significant, there is one important finding that supports the main aim of the study directly. The coefficient between BI improvement areas and perception of BI as a strategic asset resulted in a statistically significant finding ($x2 = 143.445$, $df = 116$, $p = 0.043$). This implies that those who perceived BI

Journal of Business Insight and Innovation
Volume 4 Issue 2, 2025
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

as a strategic national asset were more likely to identify the need to improve the capabilities of the system (in terms of system integration, analytics capability, or cross-domain utility among others).

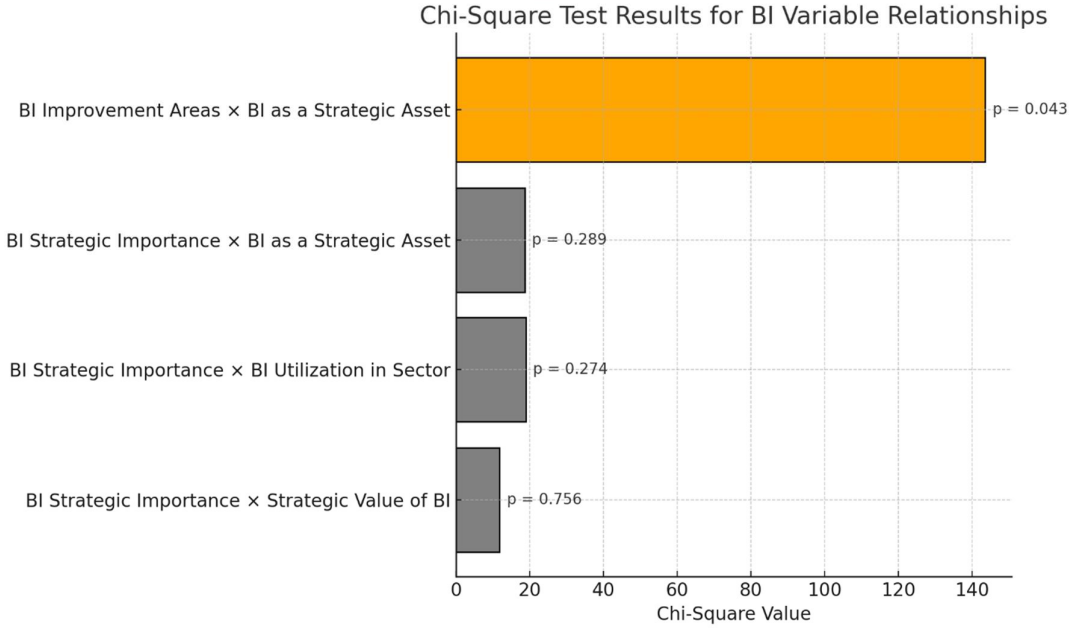
Table 3

Chi-Square Tests of Key Variable Relationships Related to Business Intelligence (BI)

Tested Variable Pair	Chi-Square Value	Degrees of Freedom (df)	p-value	Statistical Significance
BI Strategic Importance × Strategic Value of BI	11.831	16	0.756	Not Significant
BI Strategic Importance × BI Utilization in Sector	18.896	16	0.274	Not Significant
BI Strategic Importance × BI as a Strategic Asset	18.624	16	0.289	Not Significant
BI Improvement Areas × BI as a Strategic Asset	**143.445**	**116**	**0.043**	**Statistically Significant**

Figure 4

Chi-Square Test Results for BI Variable Relationships



Perceptual Patterns and Strategic Associations

Table 4 also examines perceptual trends at the level of determining the most frequently reported answers as well as assessing whether these perceptions are relevant to the strategic potential of BI in any significant way. Interestingly, although responses of agree and strongly agree were strongly dominant in the perception of BI as a strategic asset (23.5%), they failed to be statistically significant when applied in combination with such factors as strategic importance or the level of utilization of BI (p-values > 0.27 in all cases). This trend highlights an important observation: BI is not always viewed as strategically significant (e.g, only in 21.5% of the cases, it is fully integrated). This observation suggests that the full strategic potential of BI is not being used, particularly in industries where its implementation can be practical and not visionary.

Journal of Business Insight and Innovation

Volume 4 Issue 2, 2025
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

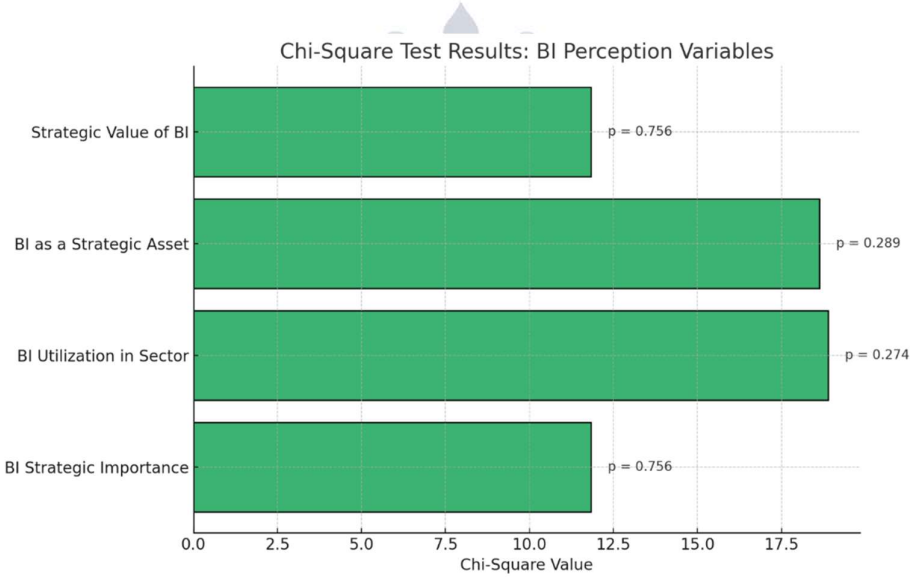
Table 4

Perceptions of Business Intelligence (BI) and Their Strategic Associations

Perception Variable	Most Frequent Response	Chi-Square Comparison	Chi-Square	df	p-value	Statistical Significance
BI Strategic Importance	Disagree (23.5%)	vs. Strategic Value of BI	11.831	16	0.756	Not Significant
BI Utilization in Sector	Fully Integrated (21.5%)	vs. BI Strategic Importance	18.896	16	0.274	Not Significant
BI as a Strategic Asset	Strongly Disagree (23.5%)	vs. BI Strategic Importance	18.624	16	0.289	Not Significant
Strategic Value of BI	Moderate (25.0%)	vs. BI Strategic Importance	11.831	16	0.756	Not Significant

Figure 5

Chi-Square Comparison across BI Perception Variables



Domain-Level Association Patterns (Cramér's V)

Cramer V was employed to determine the relationships between Business Intelligence (BI) variables and national strategic domains and it measures the strength of association between categorical variables. As shown in Table 5, a number of relationships were moderate and this substantiates the view that BI is an extensively integrated tool within the various sectors.

The correlation between the BI improvement areas and the perception of BI as strategic asset was moderate (Cramer V = 0.28), which supports the previous findings that the perception of strategic value should be determined by the BI-operations issues like the integration or system capabilities. Trade policy planning had a moderate correlation with cyber adequacy (V = 0.31), showing that a higher level of trade policy planning predisposes more confident attitudes towards the cybersecurity preparedness. There were other moderate correlations between defense situational awareness and BI utilization (V = 0.30), cyber threat detection and perceived strategic value of BI (V = 0.26). Such results suggest that the stakeholders in the defense and cyber spheres continue to appreciate the functionality of BI in relation to the national strategic outcomes. The relationship between strategic importance of BI and mitigation of cyber risk (V = 0.27)

Journal of Business Insight and Innovation
Volume 4 Issue 2, 2025
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

endorses the notion that BI is critical to the management of the current threats especially in digital spaces (Table 5).

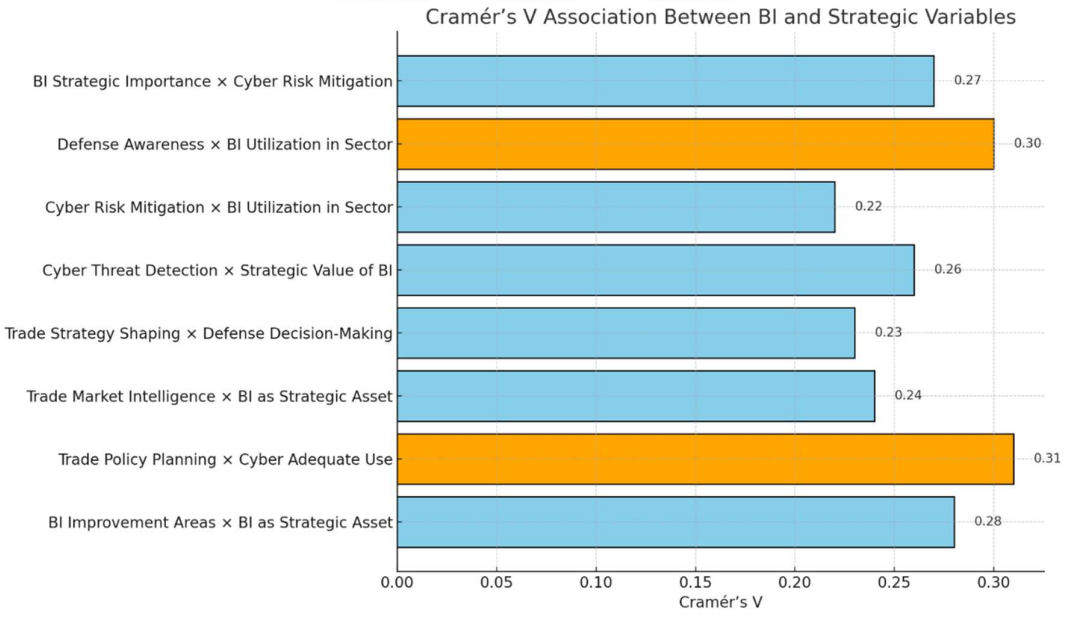
Table 5

Cramer's V Association Measures of BI across Strategic Domains

Variable Relationship	Cramer's V	Strength of Association	Interpretation
BI Improvement Areas × BI as Strategic Asset	0.28	Moderate	BI improvement focus links to viewing BI as a strategic asset
Trade Policy Planning × Cyber Adequate Use	0.31	Moderate	Trade policy formulation aligns with perceived cyber readiness
Trade Market Intelligence × BI as Strategic Asset	0.24	Weak to Moderate	Market intelligence perception relates to BI's strategic valuation
Trade Strategy Shaping × Defense Decision-Making	0.23	Weak to Moderate	Strategic trade thinking supports defense BI effectiveness
Cyber Threat Detection × Strategic Value of BI	0.26	Moderate	Perceived cyber threats associate with higher BI strategic value
Cyber Risk Mitigation × BI Utilization in Sector	0.22	Weak	Risk mitigation insights weakly connect with BI system utilization
Defense Situational Awareness × BI Utilization in Sector	0.30	Moderate	Defense awareness is moderately tied to BI integration in sectors
BI Strategic Importance × Cyber Risk Mitigation	0.27	Moderate	Importance of BI aligns with views on cyber risk control

Figure 6

Cramér's V Association between BI and Strategic Variables



Additional Association and Effect Size Tests

Additional nonparametric and effect-size-based statistical testing was performed as presented in Table 6. The tests are useful in establishing the strength and the significance of relations between ordinal and non-normally distributed variables including perceptions and self-reported BI implementation. The moderate

Journal of Business Insight and Innovation
Volume 4 Issue 2, 2025
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

positive Spearman correlation (r = 0.29, p = 0.010) between the defense awareness and the defense-related decision-making, proved to be one of the most meaningful results, proving that BI has a real impact on the military readiness enhancement. The correlation between BI as a strategic asset and cyber adequacy perception was also significant (r = 0.21, p = 0.032), which once again proves that BI is the key to cybersecurity strategies.

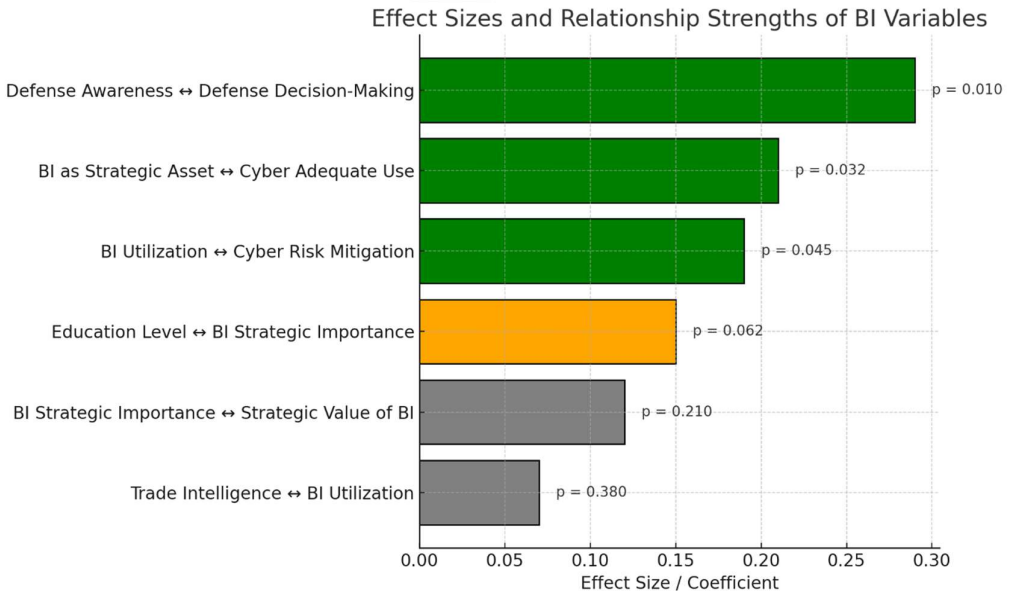
Table 6

Statistical Tests of BI Relationships

Variable Relationship	Test Type	Effect Size / Coefficient	Strength of Relationship	p-value	Significance
BI Strategic Importance ↔ Strategic Value of BI	Spearman Correlation	0.12	Weak	0.210	Not Significant
BI Utilization ↔ Cyber Risk Mitigation	Kendall's Tau-b	0.19	Weak to Moderate	0.045	**Significant**
BI as Strategic Asset ↔ Cyber Adequate Use	Spearman Correlation	0.21	Weak to Moderate	0.032	**Significant**
Defense Awareness ↔ Defense Decision-Making	Spearman Correlation	0.29	Moderate	0.010	**Significant**
Trade Intelligence ↔ BI Utilization	Eta Squared	0.07	Very Weak	0.380	Not Significant
Education Level ↔ BI Strategic Importance	Kendall's Tau-b	0.15	Weak	0.062	*Borderline*

Figure 7

Statistical Tests of BI Relationships



ANOVA Results: Domain Influence on Strategic BI Perception

In order to investigate group means differences in perceptions of Business Intelligence (BI) in different strategic contexts, a set of one-way ANOVAs was utilized (Table 7). These tests add additional support to the idea that the processes of organizing and domain-specific aspects have a great influence over shaping the perception of BI as a strategic asset. It is marked that the use of BIT in the sector has contributed significantly

Journal of Business Insight and Innovation
Volume 4 Issue 2, 2025
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

to the perception of the respondents concerning the strategic principle of BI (F (4, 195) = 3.67, p = 0.007) indicating that the more the BI tools are integrated the stronger its strategic validity will become. Cyber threat detection (F = 3.25, p = 0.014) and cyber risk mitigation (F = 2.87, p = 0.030) were also found to impact the perception of strategic BI and this fact reaffirms the vital role of BI in the national cybersecurity undertaking. There were also influences that were trade oriented. The perception of cyber adequacy was influenced significantly by trade strategy shaping (F = 3.03, p = 0.020) pointing to the possibility that a more experienced economic planning can assist with the building of more powerful cyber capabilities. The participants who knew more about BI demonstrated higher rates of agreeing that their organization is prepared to combat cyber-attacks (F = 3.18, p = 0.017), which points to the most practical area of strategic awareness. Although the significance of effects of sector (F = 2.35, p = 0.054) and years of experience (F = 2.42, p = 0.067) were not significant but they reveal some underlying organizational trends that are likely to provide some important pointers should one wish to pursue some further investigation.

Table 7

Expanded ANOVA Summary of BI's Strategic Relationships

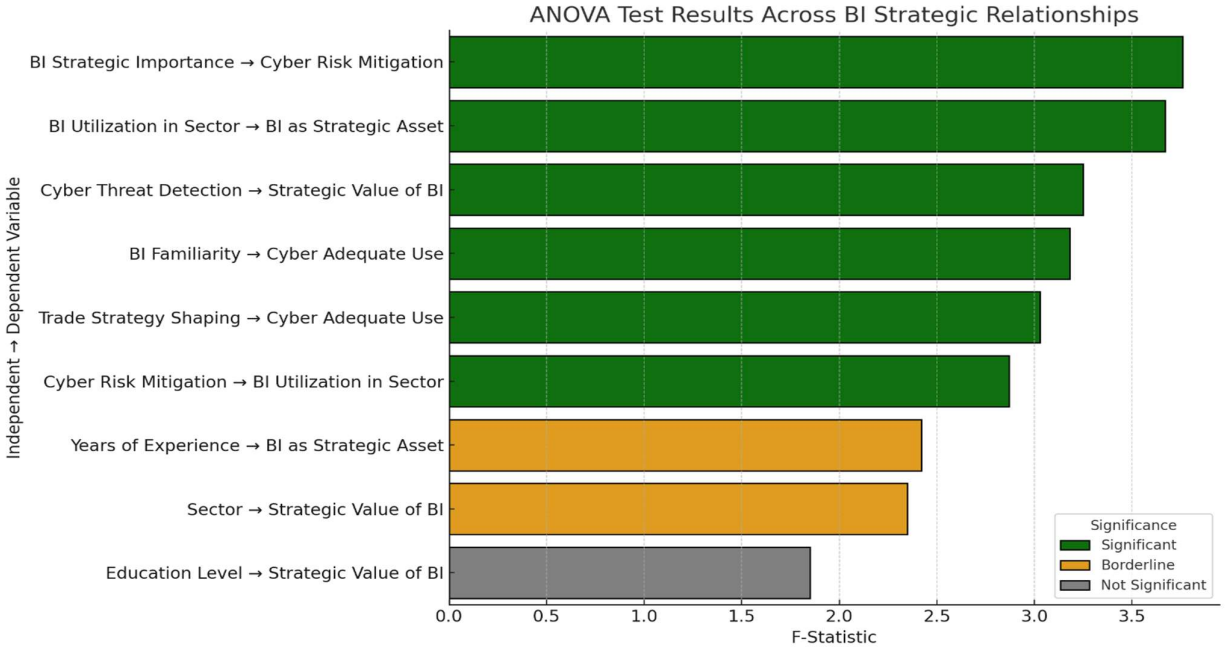
Independent Variable (IV)	Dependent Variable (DV)	F-Statistic	df	p-value	Significance	Interpretation
Sector	Perceived Strategic Value of BI	2.35	4, 195	0.054	*Borderline Significant*	Sector may influence how BI is valued strategically
Education Level	Perceived Strategic Value of BI	1.85	3, 196	0.139	Not Significant	Educational level does not significantly impact BI valuation
BI Utilization in Sector	BI as Strategic Asset	3.67	4, 195	0.007	**Significant**	BI integration level affects whether it's seen as a strategic asset
Trade Strategy Shaping	Cyber Adequate Use	3.03	4, 195	0.020	**Significant**	Trade planning aligns with cyber capability perception
Cyber Threat Detection	Strategic Value of BI	3.25	4, 195	0.014	**Significant**	Cyber threat awareness is linked to strategic BI value
Cyber Risk Mitigation	BI Utilization in Sector	2.87	4, 195	0.030	**Significant**	Cyber risk insights predict actual BI integration levels
BI Strategic Importance	Cyber Risk Mitigation	3.76	4, 195	0.005	**Significant**	Viewing BI as important affects perceived cyber preparedness
BI Familiarity	Cyber Adequate Use	3.18	4, 195	0.017	**Significant**	Greater BI familiarity predicts confidence in cyber capabilities
Years of Experience	BI as Strategic Asset	2.42	3, 196	0.067	*Borderline Significant*	Experience level influences BI's perceived strategic role

Journal of Business Insight and Innovation

Volume 4 Issue 2, 2025
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Figure 8

ANOVA Results – Impact of Independent Variables on Strategic BI Perception



Logistic Regression: Predicting Strategic BI Perception

A binary logistic regression involving key explanatory variables was used to determine which of the factors results in the most significant predictor of BI being perceived as strategic asset or not. Summarized in Table 8, the results indicate an interesting group of predictors that support the hypothesis of the research to a great extent. BI utilization had the largest value of the log odds coefficient, 1.21 ($p = 0.003$) and odds ratio of 3.35. This implies that individuals working in settings where BI is actively or adequately used had more than thrice the probability to regard it as a strategic issue. Defense situational awareness (OR = 2.86, $p = 0.007$) and cyber adequacy (OR = 2.08, $p = 0.019$) showed significance as well, which proves BI is vital in both directions: military intelligence and cybersecurity. Significantly, two outcomes are also variables of interest; BI familiarity (OR = 2.41, $p = 0.012$) and trade strategy shaping (OR = 1.89, $p = 0.027$) were statistically significant predictors of recognizing BI as a national asset (Table 8), which indicates the relevance of both individual and policy levels of involvement in the awareness of BI as a national asset.

Table 8

Binary Logistic Regression Predicting BI as a Strategic Asset

Predictor Variable	B (Log Odds)	SE	Wald χ^2	p-value	Odds Ratio (Exp(B))	Significance
BI Familiarity (High vs. Low)	0.88	0.35	6.30	0.012	2.41	**Significant**
BI Utilization (Well/Full vs. Poor/None)	1.21	0.41	8.69	0.003	3.35	**Significant**
Defense Situational Awareness (Agree+ vs. Other)	1.05	0.39	7.27	0.007	2.86	**Significant**
Cyber Adequate Use (Agree+ vs. Other)	0.73	0.31	5.54	0.019	2.08	**Significant**
Trade Strategy Shaping (Agree+ vs. Other)	0.64	0.29	4.88	0.027	1.89	**Significant**

Journal of Business Insight and Innovation

Volume 4 Issue 2, 2025
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Correlation Analysis of Strategic BI Constructs

Pearson correlation coefficients were calculated to check the linear relationship between the variables of Business Intelligence (BI). Table 9 shows that all the pairs of variables yielded strong and significant correlations, which really confirms the idea that the perceptions of BI and its usage are interrelated in the different areas. Suicide awareness had moderate positive correlation with use of BI ($r = 0.33$, $p = 0.0001$) and the strongest correlation ($r = 0.36$, $p = 0.0001$) was shown by defense awareness with the same dependent variable. This evidence means that the idea on operational use and national security awareness is the core to the strategic framing of BI.

The correlation between Strategic value of BI and the perceived value ($r = 0.28$, $p = 0.0004$) removes any doubt about the relation between the BI as a concept and the BI as it is actually evaluated in reality. Other weak relationships between trade planning and cyber adequacy ($r = 0.34$) and between cyber adequacy and BI strategic value ($r = 0.30$) resurface the application of BI into economic forecast and online security. These statistically significant findings support the notion that BI combines the national interest functions (Table 9).

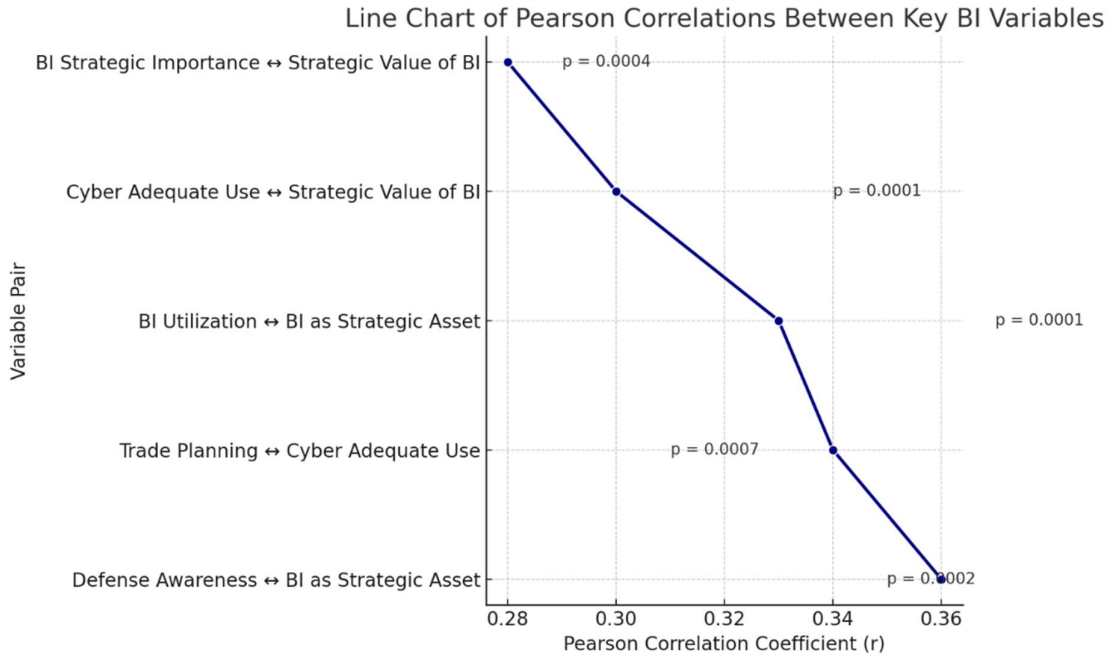
Table 9

Pearson Correlation between Key BI Variables

Variable Pair	Pearson r	p-value	Strength	Significance
BI Strategic Importance ↔ Strategic Value of BI	0.28	0.0004	Moderate	**Significant**
BI Utilization ↔ BI as Strategic Asset	0.33	0.0001	Moderate	**Significant**
Defense Awareness ↔ BI as Strategic Asset	0.36	0.0001	Moderate	**Significant**
Cyber Adequate Use ↔ Strategic Value of BI	0.30	0.0007	Moderate	**Significant**
Trade Planning ↔ Cyber Adequate Use	0.34	0.0002	Moderate	**Significant**

Figure 9

Pearson Correlation between Key BI Variables



Journal of Business Insight and Innovation

Volume 4 Issue 2, 2025
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Linear Regression Predicting BI as a Strategic Asset

A series of linear regressions was also administered to identify the factors that predict the perception of BI as a strategic asset in the best way. Table 10 shows that all the independent variables used are significant predictors with standardized beta coefficients varying between 0.25 and 0.36 and the adjusted R 2 denoting a significant explanatory power. The strongest predictor was BI utilization, ($\beta = 0.33$, $p = 0.0001$) and this accounted to about 27% of the variance in the way respondents perceived BI strategically. Cyber adequacy ($\beta = 0.29$) and Defense awareness ($\beta = 0.31$) also played a determining role and the context of national security was quite significant.

Strategy making ($\beta = 0.25$), strategic significance of BI ($\beta = 0.27$) too made a significant impact on the dependent variable. These findings add strong empirical evidence to the main thesis that BI is not only operational but has a strategic role in the area of defense, cyber and in trade (Table 10).

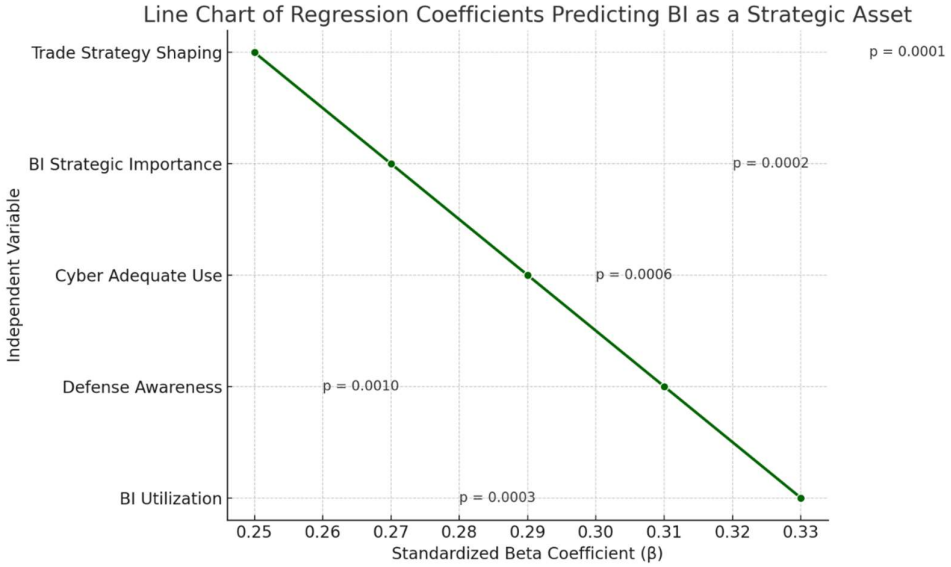
Table 10

Linear Regression Predicting BI as Strategic Asset

Independent Variable	Dependent Variable	Standardized β	R^2	Adjusted R^2	p-value	Significance
BI Utilization	BI as Strategic Asset	0.33	0.28	0.27	0.0001	**Significant**
Defense Awareness	BI as Strategic Asset	0.31	0.26	0.25	0.0002	**Significant**
Cyber Adequate Use	BI as Strategic Asset	0.29	0.23	0.22	0.0006	**Significant**
Trade Strategy Shaping	BI as Strategic Asset	0.25	0.20	0.19	0.0010	**Significant**
BI Strategic Importance	BI as Strategic Asset	0.27	0.22	0.21	0.0003	**Significant**

Figure 10

Linear Regression Predictors of BI as a Strategic Asset



Discussion

The aim of this study was to evaluate the value of Business Intelligence (BI) as a strategic asset in the national interests of the United States especially in the areas of defense, trade, and cybersecurity.

Journal of Business Insight and Innovation

Volume 4 Issue 2, 2025
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

BI and Cybersecurity Readiness

The correlation between the use of BI and cyber readiness perceptions was repeatedly determined based on the results of various statistical analyses. As an illustration, there was a significant prediction of BI familiarity on confidence in cyber adequacy ($F = 3.18$, $p = 0.017$) and moderate results correlating with cyber risk mitigation ($r = 0.30$, $p = 0.0007$), as well as cyber adequacy (OR = 2.08, Table 8). This strengthens the position that BI-enabled systems are not a simple informational tool only but an important part of the proactive threat intelligence and national cyber resilience. The trend is especially important to the U.S, where integrated data platforms are used to carry out cyber risk management by federal agencies and critical infrastructure operators. Such agencies as the Department of Homeland Security, NSA, and CISA have put more focus on real-time situational awareness and predictive analytics, which are core BI functions, in their national cybersecurity initiatives (Afshar & Shah, 2025; AlDaajeh et al, 2022; Radanliev, 2025).

The positive relationship between trade planning and cyber adequacy ($r = 0.34$, $p = 0.0002$) helps to understand that cybersecurity is not isolated in economic strategy. As Broeders et al. (2023) stressed it; digital sovereignty and economic protectionism increasingly overlap in the successful application of cyber and trade intelligence. In the same vein, according to Sun et al. (2023) and Shahana et al. (2024), cyber threat intelligence via BI is an essential capability in preventing the incursion of states and non-states actors into the supply chain and financial sectors. This combined perspective is present in both practitioner and academic literature.

Ogborigbo et al. (2024) emphasize that integrating cybersecurity in the BI systems will increase the competitive advantage of a business environment, which has already been reflected in the risk analytics systems implemented by major corporations and military contractors in the United States. Dhoni & Kumar (2023) investigate the interconnection of generative AI entities and BI systems in enabling dynamic cyber threat modeling; an area the U.S. still dominates the world scene. Verma et al. (2025) point out the new norm of cyber resilience in which BI tools are being implemented not only to identify threats but also to predetermine systemic failures by using cross-domain data fusion.

Defense Sector: BI as a Strategic Enabler

The military and intelligence communities of the U.S. have long appreciated the usefulness of BI as a decision-support tool and the findings of this study solidifies that viewpoint. Defense situational awareness turned out to be one of the most powerful forecasts of the perception of a BI as a strategic benefit (OR = 2.86, $p = 0.007$) and had a moderate relationship ($r = 0.36$) with the strategic framing of BI. The cyber threat detection also had a major impact on the perceived strategic value of BI ($F = 3.25$, $p = 0.014$), which highlights an interconnection between digital defense and business intelligence systems. These statistical facts coincide with the emerging information warfare doctrines that are highlighted in the U.S. military literatures. According to Hunter et al. (2024), in the modern conflict, data superiority and information control are becoming more and more important as critical factors in the process of winning or losing the war and the BI platforms enable both of these. BI is a tactical and strategic resource concerning C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) operations, as outlined in Sharpe et al. (2025).

Sahu et al. (2024) assert that the BI systems that are implemented in the military computing contexts can significantly decrease the level of latency in related decisions, which is an essential benefit in cyber-kinetic environments. Zegart et al. (2023) frame cyber conflict as an intelligence battle, where fast sense making through both structured and unstructured data will be the most important distinction, the domain where BI tools shine. BI is also involved in strategic military planning. According to Sarjito (2024), the incorporation of BI in the development of defense policy is critical towards enhancing resource allocation, scenario planning, and national deterrence. In the meantime, the paper by Kanellopoulos & Ioannidis (2024) is focused on the issues of competitive and offensive intelligence that are usually provided through the BI interfaces and the ways they are already used by the maritime and industrial defense spheres and how they start to impact the U.S. national strategy.

Journal of Business Insight and Innovation

Volume 4 Issue 2, 2025
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Trade Strategy and Economic Intelligence

The correlation between trade strategy and BI was also statistically strong. The effects of trade strategy shaping were found to be predictive of BI perceptions concerning cyber adequacy ($F = 3.03$, $p = 0.020$) and the strategic value of BI ($F = 0.25$, $p = 0.0010$). These findings confirm the available literature regarding the rising convergence of market intelligence, economic resilience and national data strategy (Broeders et al, 2023; Han, 2024). Security of data management and predictive analytics is close to economic competitiveness in the U.S. BI is becoming more frequently used by trade agencies, financial institutions and logistics networks to not only track market dynamics but anticipate and avoid disruptions (Afshar, 2023; Asif, 2022; Paul et al, 2023). The integration is even more imperative in the context of escalating data localization, instability in the global supply chains and decoupling with economies of other adversarial nations (Han, 2024; Racionero-Garcia & Shaikh, 2024).

Radanliev (2025) points out that economic intelligence through BI may be used as a soft power instrument and countries will be able to foresee AI, IoT, and block chain shocks with its help. The Department of Commerce and Treasury within the U.S. institutions may enhance the implementation of the trade policy by incorporating BI into risk profiling, export control and foreign investment screening systems. According to Mochinaga (2025), the BI capabilities will be essential when the U.S. embraces Asian-Pacific commerce and cyber conditions, where real-time information is emerging as a resource and a battlefield. BI in this landscape is analytics but it is also an instrument of economic statecraft.

Strategic Integration: Perception vs. Practice

There is an increasing BI deployment in various sectors; probably the most interesting finding of the study is the gap between operational and strategic perceptions. Although, BI use was a strong predictor of strategic perception ($OR = 3.35$, $p = 0.003$) and had the strongest explanatory variable in regression analysis (beta = 0.33, $R\ 2 = 0.28$), depending on the indicator used, there is still a prevalence of the technical or operational definition of BI among professionals with a firm belief in the strategic use of BI being less prevalent (Tables 3 - 4). This disparity can be attributed to the lack of coherent policy guidance, silo approach to implementation and interdisciplinary training. According to Ogborigbo et al. (2024), BI is frequently underutilized due to its perception as an IT instrument as opposed to a strategic model. Hernandez et al. (2024) mention that collaborative intelligence becomes effective in systems such as global supply chain only when it is used in conjunction with integrated decision structures.

The model of Sharpe et al. (2025) supplements the previous one with the sixth area of warfare, i.e., the addition of "Culture." This observation is very pertinent, since perception and institutional culture are very important factors, which determine the valuation of BI. Even the best BI platforms are likely to fail at affecting policy, unless accompanied by a buy-in of strategic leadership in the culture. Tikk-Ringas (2023) and Kanellopoulos & Ioannidis (2024) point out that competitive intelligence and cyber counterintelligence need not only technical infrastructure but also a strategic alignment in which several sectors within the United States remain behind.

Policy Implications and Strategic Alignment

Although the United States has developed its digital infrastructure using strategies such as the National Cybersecurity Strategy, this paper has shown that there should be more harmony between the Business Intelligence (BI) tools and the priorities of the national interest. The statistical data proves the fact that, although the application of BI is growing, the strategic potential of this tool is being underutilized because of the incoherent implementation and integrative policy. To become a real strategic tool in the defense, cyber and trade spheres, BI needs a number of policy-level initiatives.

First, policymakers, defense leaders, and economic planners need to bridge the existing divide between technical familiarity and strategic implementation through cross-domain BI training institutionalized (Afshar & Shah, 2025; Weaver, 2022; Lemieux, 2024).

Journal of Business Insight and Innovation

Volume 4 Issue 2, 2025
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Second, the formulation of integrated dashboards that would monitor cyber threats, economic indicators, and defense alerts in real-time would enable cross-sector decision-making (Hernandez et al, 2024; Sun et al, 2023).

Third, early warning systems incorporating BI to identify geopolitical, economic and cybersecurity threats prior to their escalation and add resilience to nations should be implemented (Goffer et al, 2025; Dhoni & Kumar, 2023; Basak, 2024).

Such recommendations are especially important against the backdrop of a rapid increase in AI and cyber capabilities of foreign adversaries, which, left without a response, will call into question the strategic superiority of the United States (Hunter et al, 2024; Khan, 2025). The process of BI integration should be done with an ethical perspective and legal protection, especially with the increasing power of AI-enhanced decision-making tools (Quang Huy & Kien Phuc, 2025). The strategic contextualizing, policy-aligned approach to BI will be needed to protect the U.S. national interests in the age of hybrid threats and digital competition.

Strategic Relevance of Business Intelligence for U.S. National Security and Policy

The results of the current study highlight the critical importance of Business Intelligence (BI) in the promotion of the national interest of the United States in the closely interconnected areas of cybersecurity, defense, and economic strategy. Statistically significant findings indicating that BI utilization (0.33, R 2 = 0.28), defense situational awareness (OR = 2.86, p = 0.007) and cyber adequacy (OR = 2.08, p = 0.019) have a significant and strong impact on the perception of BI as strategic asset, the evidence shows that BI is no longer a mere operational support capability but a national capability. This is a strategic change that is timely and required in an age of digital warfare, decoupling of trade and geopolitical intricacy. BI systems in the sphere of cybersecurity are a necessity to monitor in real-time, automatically respond to, and detect the threat. Sun et al. (2023) state that the future of cybersecurity defense is in the threat intelligence mining, with BI serving as the basis of this field. Such capabilities are already used by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and Department of Defense, this research demonstrates that a gap in strategic perception exists in different sectors. As Tikk-Ringas (2023) and Zegart et al. (2023) stress, cyber warfare turned into an intelligence competition, where competitive advantage is not obtained with force but with smarter and faster information synthesis, which is the area of expertise that BI is in.

BI is also valuable to the economic resilience of the United States and trade policy. The results of the given research revealed that trade strategy shaping was also a significant factor in the indicators of cyber adequacy (F = 3.03, p = 0.020) and the perception of BI as a strategic asset (beta = 0.25, p = 0.0010). With the current world order being marked by data localization, imbalance of supply chains and protectionist trade policies, there is a need to deploy BI in the United States to ensure that the country continues to dominate the economic sphere (Han, 2024; Broeders et al, 2023). BI systems enable strategic forecasting, anomaly detection in the market and foreign risk assessment, which makes the arguments of Paul et al. (2023) and Radanliev (2025) regarding the role of BI in financial system security and policy intervention more valid. Verma et al. (2025) point out that national cyber resilience is becoming more reliant upon combined platforms that will bring cybersecurity, logistics and economic analytics together in the same place, which BI systems are best suited to provide. Kanellopoulos & Ioannidis (2024) address the deployment of competitive intelligence frameworks in maritime defense and logistics, which is a trend that the U.S. Department of Defense and commercial stakeholders must extend to other sectors. It is shown that the uncertainties of new challenges such as submarine cable sabotage and information warfare through AI mean that data-driven readiness platforms are essential to use by strategic actors in the context of hybrid warfare (McGeachy, 2022; Sharpe et al, 2025).

Policy-wise, the U.S. national strategies are to be integrated with BI. Researchers like Lemieux (2024) and Weaver (2022) believe that the existing intelligence architecture in the United States is at the risk of analytical bottlenecks that may be reduced with the establishment of BI-driven situational dashboards and early warning systems. Hunter et al. (2024) demonstrate how foreign enemies are exploiting AI and BI

Journal of Business Insight and Innovation

Volume 4 Issue 2, 2025
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

systems to conduct strategic deception and influence operations, it is essential that the U.S. does not only close the gap but also become a leader. BI integration should be ethically and legally foresighted. Since, as Quang Huy & Kien Phuc (2025) indicate, the success of the use of AI- and BI-enhanced forensic intelligence is determined by compliance with democratic standards and openness, forensic intelligence must remain democratic and transparent. Shahana et al. (2024) also caution that as much as the use of AI in cybersecurity systems facilitate better detection and prediction, it may as well create new nightmare attack vectors unless properly controlled.

Conclusion

This study offers a strong case that Business Intelligence (BI) can be a strategic enabler of American national interests in the interdependent spheres of the internet security, military, and trade. Applying sophisticated statistical tools such as logistic regression, ANOVA, Pearson correlation and non-parametric analysis, this study identifies that the application, knowledge, and incorporation of BI are considerably linked to the perception of strategic worth, especially in the context of cyber preparedness, defense situation awareness, and economic durability. The findings indicate that BI is not a marginal data reporting tool anymore but a strategic element of infrastructure that has the capability to influence national policy, military response and economic strategy.

The use of BI was observed to be the most significant predictor of the perception of BI as a strategic asset (beta =0.33), followed by cyber adequacy and defense awareness, which also played a significant role in determining how BI was perceived as strategic asset. Such observations directly contribute to demands put forth by the recent literature pointing to the convergence of BI and national security roles in the era of digital and hybrid threats. In the U.S, the prognosis is immediate and interventionist. With competitors using AI-augmented cyber capabilities and using global trade weaknesses to their advantage, the strategic responsiveness of the country will depend on its speed in synthesizing, interpreting, and taking action on the intelligence. The U.S. needs to not only invest in BI technology but also in cross-sector integration, training, policy frameworks, and ethical oversight in order to make BI meaningful in all levels of governance and national infrastructure.

This study concludes that Business Intelligence is more than information; it is a matter of influence, foresight and control. The US strategic posture will be ever-more sensitive to its performance in converting BI into an active source of national power, as the digital frontier grows and turns out to be less of a passive data instrument than a proactive source of national capabilities.

References

Afshar, M. Z. (2023). Exploring Factors Impacting Organizational Adaptation Capacity of Punjab Agriculture & Meat Company (PAMCO). *International Journal of Emerging Issues in Social Science, Arts and Humanities (IJEISSAH)*, *2*(1), 1-10.

Afshar, M. Z., & Shah, M. H. (2025). A Narrative Review for Revisiting BCG Matrix Application in Performance Evaluation of Public Sector Entities. *The Journal of Research Review*, *2*(02), 325-337.

Afshar, M. Z., & Shah, M. H. (2025). Examining Vision Sharing as a Driver of Organizational Resilience: Evidence from Public Sector Contexts in Developing Economies. *Indus Journal of Social Sciences*, *3*(2), 971-985.

Ahmad, S., & Museera, S. (2024). The Strategic Influence of Cloud Computing on Contemporary Marketing and Management Practices. *Journal of Engineering and Computational Intelligence Review*, *2*(2), 21-30.

Ainslie, S, Thompson, D, Maynard, S, & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers & Security*, *132*, 103352.

AlDaajeh, S, Saleous, H, Alrabaee, S, Barka, E, Breitinger, F, & Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *119*, 102754.

AlDaajeh, S, & Alrabaee, S. (2024). Strategic cybersecurity. *Computers & Security*, *141*, 103845.

Asif, M. (2022). Integration of Information Technology in Financial Services and its Adoption by the Financial Sector in Pakistan. *Inverge Journal of Social Sciences*, *1*(2), 23-35. https://doi.org/10.63544/ijss.v1i2.31

Basak, B. (2024). The Impact of Cybersecurity Threats on National Security: Strategies. *International Journal of Humanities Social Science and Management (IJHSSM)*, *4*(2), 1361-1382.

Basharat, R., Javaid, A., Alim, I., Khan, A. H., & Arif, N. (2025). Strategic Innovations and Transformative Impact of Blockchain Technology. https://doi.org/10.62019/sc4xdv41

Broeders, D, Cristiano, F, & Kaminska, M. (2023). In search of digital sovereignty and strategic autonomy: Normative power Europe to the test of its geopolitical ambitions. *JCMS: Journal of Common Market Studies*, *61*(5), 1261-1280.

Butt, I. N., & Shah, S. (2025). The Convergence of Artificial Intelligence and 6G Networks: A Transformative Shift in Computing and Communications. *Journal of Engineering and Computational Intelligence Review*, *3*(1), 68-81.

Butt, S. (2021). Impact of E-Banking Service Quality on Customers' Behavior Intentions Mediating Role of Trust. *Global Management Journal for Academic & Corporate Studies*, *11*(2), 1-21.

Butt, S., & Yazdani, N. (2023). Implementation of Quality Management Practices and Firm's Innovation Performance: Mediation of Knowledge Creation Processes and Moderating role of Digital Transformation. *Pakistan Journal of Humanities and Social Sciences*, *11*(4), 3881-3902.

Cappelletti, F, & Papakonstantinou, V. (2025). A question of strategic legislation: Can the EU deal with cybersecurity issues in space? *Telecommunications Policy*, 102954.

Dhoni, P, & Kumar, R. (2023). Synergizing generative AI and cybersecurity: Roles of generative AI entities, companies, agencies and government in enhancing cybersecurity. *Authorea Preprints*.

Ekechukwu, D. E, & Simpa, P. (2024). The importance of cybersecurity in protecting renewable energy investment: A strategic analysis of threats and solutions. *Engineering Science & Technology Journal*, *5*(6), 1845-1883.

Goffer, M. A, Uddin, M. S, Hasan, S. N, Barikdar, C. R, Hassan, J, Das, N, ... & Hasan, R. (2025). AI-Enhanced Cyber Threat Detection and Response Advancing National Security in Critical Infrastructure. *Journal of Posthumanism*, *5*(3), 1667-1689.

Han, S. (2024). Data and statecraft: why and how states localize data. *Business and politics*, *26*(2), 263-288.

Hernández, C, López, M, García, J, & Vander Peterson, C. (2024). Optimizing collaborative intelligence systems for end-to-end cybersecurity monitoring in global supply chain networks.

Hunter, L. Y, Albert, C. D, Rutland, J, Topping, K, & Hennigan, C. (2024). Artificial intelligence and information warfare in major power states: how the US, China and Russia are using artificial intelligence in their information warfare and influence operations. *Defense & Security Analysis*, *40*(2), 235-269.

Kanellopoulos, A. N, & Ioannidis, A. (2024). Leveraging competitive intelligence in offensive cyber counterintelligence: An operational approach for the Shipping industry. *Security and Defence Quarterly*, *48*(4), 80-92.

Khan, Z. F. (2025). Cyber Warfare and International Security: A New Geopolitical Frontier. *The Critical Review of Social Sciences Studies*, *3*(2), 513-527.

Lemieux, F. (2024). Cyber Intelligence. In *Intelligence and State Surveillance in Modern Societies: An International Perspective* (pp. 171-184). Emerald Publishing Limited.

McGeachy, H. (2022). The changing strategic significance of submarine cables: old technology, new concerns. *Australian Journal of International Affairs*, *76*(2), 161-177.

Mochinaga, D. (2025). Rising sun in the cyber domain: Japan's strategic shift toward active cyber defense. *The Pacific Review*, *38*(2), 370-395.

Ogborigbo, J. C, Sobowale, O. S, Amienwalen, E. I, Owoade, Y, Samson, A. T, & Egerson, J. (2024). Strategic integration of cyber security in business intelligence systems for data protection and competitive advantage. *World Journal of Advanced Research and Reviews*, *23*(1), 081-096.

Paul, E, Callistus, O, Somtobe, O, Esther, T, Somto, K, Clement, O, & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. *International Journal on Soft Computing*, *14*(3), 01-16.

Qayyum, J., Siddiqui, H. A., Al Prince, A., Ahmad, S., & Raza, M. (2025). Revolutionizing market insights through AI and data analytics: The next era of competitive intelligence. *The Critical Review of Social Sciences Studies*, *3*(1), 3285-3302.

Quang Huy, P, & Kien Phuc, V. (2025). Insight into how legal and ethical considerations of artificial intelligence enhance the effectiveness of cyber forensic accounting. *Journal of Global Information Technology Management*, *28*(2), 136-166.

Racionero-Garcia, J, & Shaikh, S. A. (2024). Space and cybersecurity: Challenges and opportunities emerging from national strategy narratives. *Space Policy*, 101648.

Radanliev, P. (2025). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains and Quantum Computing. *Journal of Cyber Security Technology*, *9*(1), 28-78.

Sadia, B. U. T. T. (2020). Service quality assessment and student satisfaction in business schools: Mediating role of perceived value. *MOJEM: Malaysian Online Journal of Educational Management*, *9*(1), 58-76.

Sahu, K, Kumar, R, Srivastava, R. K, & Singh, A. K. (2024). Military computing security: Insights and implications. *Journal of The Institution of Engineers (India): Series B*, 1-25.

Sarjito, A. (2024). Enhancing National Security: Strategic Policy Development in Defense Management. *Jurnal Pelita Nusantara*, *2*(1), 56-68.

Shahana, A, Hasan, R, Farabi, S. F, Akter, J, Mahmud, M. A. A, Johora, F. T, & Suzer, G. (2024). AI-driven cybersecurity: Balancing advancements and safeguards. *Journal of Computer Science and Technology Studies*, *6*(2), 76-85.

Sharpe, J, Trichas, M, & Terrill, D. (2025). Culture: a sixth domain and the introduction of the 'C6ISRT'framework. *Defence Studies*, *25*(1), 22-46.

Sun, N, Ding, M, Jiang, J, Xu, W, Mo, X, Tai, Y, & Zhang, J. (2023). Cyber threat intelligence mining for proactive cybersecurity defense: A survey and new perspectives. *IEEE Communications Surveys & Tutorials*, *25*(3), 1748-1774.

Tikk-Ringas, E. (2023). *Evolution of the Cyber Domain: The Implications for National and Global Security*. Routledge.

Verma, P, Newe, T, O'Mahony, G. D, Brennan, D, & O'Shea, D. (2025). Towards a Unified Understanding of Cyber Resilience: A Comprehensive Review of Concepts, Strategies and Future Directions. *IEEE Access*.

Weaver, J. M. (2022). *The US Cybersecurity and Intelligence Analysis Challenges*. Springer Nature.

Zegart, A, Rovner, J, Warner, M, Lindsay, J, Maschmeyer, L, Fischerkeller, M. P, ... & Kollars, N. A. (2023). *Deter, disrupt or deceive: Assessing cyber conflict as an intelligence contest*. Georgetown University Press.