RJOAS: Russian Journal of Agricultural and Socio-Economic Sciences
ISSN 2226-1184 (Online) | Issue 12(144), December 2023

UDC 355; DOI 10.18551/rjoas.2023-12.09

STUDY OF THE INFLUENCE OF LEGAL SECURITY AND CYBER INTELLIGENCE CAPACITY ON STRENGTHENING GOVERNANCE OF CYBER DEFENSE IN INDONESIA

Purnomo Widyanto Pudyo*
Doctoral Program of Resilience Studies, University of Brawijaya, Malang, Indonesia

Moeljadi
Faculty of Economics and Business, University of Brawijaya, Malang, Indonesia

Kusumaningrum Adi
Faculty of Law, University of Brawijaya, Malang, Indonesia

Aminuddin M. Faishal
Faculty of Social and Political Sciences, University of Brawijaya, Malang, Indonesia

*E-mail: widhi9843al@gmail.com

ABSTRACT
Stakeholders in cyber intelligence and cyber defense systems are believed to play a significant role in enhancing national resilience. The involvement of intelligence entities in the cyber domain, along with institutional and governance aspects of cyber defense, can contribute to bolstering national resilience. This study seeks to assess the impact of collaboration among cyber stakeholders on the reinforcement of cyber defense governance in Indonesia. Questionnaires were distributed to various cyber intelligence stakeholders in the country to determine whether increased collaboration has a positive effect on strengthening cyber defense governance. A quantitative approach was employed, utilizing SPSS analysis tools to measure the extent of influence between variables. The findings of the analysis reveal a correlation between legal certainty and the reinforcement of cyber defense governance, as well as a connection between capacity building and strengthening cyber defense governance. The multiple linear regression equation analysis indicates that the implementation of legal certainty and capacity building positively contributes to enhancing cyber defense governance in Indonesia.

KEY WORDS
Cyber legal certainty, SPSS, cyber defense, Indonesia.

According to Minister of Defense Regulation Number 82 of 2014, which pertains to Cyber Defense, cyberspace is characterized as a realm where communities are interconnected through networks, such as the internet, to engage in diverse daily activities. Presently, electronic systems, including internet networks, play a crucial role in facilitating a wide range of activities across business, trade, health services, communications, and government sectors. The escalating prevalence and growing reliance on information and communication technology through internet networks also come with an uptick in threat activities (Andress & Winterfeld, 2014).

Indonesia has achieved notable advancements in the digital domain in recent years. The country's standing in the current landscape of the digital world can be elucidated through several facets, starting with internet penetration. The count of internet users in Indonesia has been experiencing rapid and continual growth (Brantly, 2013). Based on the most recent data, over 70% of Indonesia's population is now connected to the internet. This statistic underscores the widespread adoption of digital technology throughout the country (Marsetio, 2016). Another significant aspect is the rapid growth of e-commerce in Indonesia. Platforms like Tokopedia, Bukalapak, and Shopee have experienced considerable success in the

Indonesian market. Millions of individuals in Indonesia utilize these platforms for online shopping, selling their products, and conducting digital transactions (Caplan, 2013).

As a nation making rapid strides in digital advancement, Indonesia is concurrently grappling with the escalating threat of cyber attacks. Among the most contemporary cyber threats in Indonesia are Ransomware attacks, Distributed Denial of Service (DDoS) attacks, Phishing attacks, Malware and Botnet attacks, and targeted attacks. A ransomware attack involves hackers encrypting user data or a computer system and then demanding a ransom payment in exchange for the decryption key. The surge in digital progress in Indonesia is paralleled by a heightened presence of threats in cyberspace, necessitating comprehensive management. In this context, security institutions and agencies, including intelligence entities, need to adopt a multidimensional approach to fulfill their responsibilities in cyberspace (David & R., 2011).

The objective of this research is to formulate a framework that enhances collaboration among cyber stakeholders to reinforce cyber defense governance in Indonesia. Employing a quantitative approach, questionnaires were distributed to various cyber intelligence stakeholders across Indonesia to discern their respective roles. Respondents were selected from regions across Indonesia, including major cities characterized by relatively high levels of cyber attacks.

Several previous studies that were used as references in this research were research with the title From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond (Zheng, 2015), research with the title Opportunities and Threats: A Security Assessment of State Egovernment Websites (Zhao, J., & Zhao, 2010), research with the title Strategic Cyber Intelligence: An examination of Practices across Industry, Government, and Military (Uthoff, 20115), research with the title Egovernment: Implementation Policies and Best Practices from Singapore (Tan & Subramaniam, 2005), research with the title Cyber Security: Perspective for A Comprehensive Approach (Roell, Peter, Lurtz, Feldt, & Thiele, 2013), research with the title Kepentingan Kebijakan Politik Luar Negeri Freedom Of Navigation Amerika Serikat Terhadap Sengketa di Laut China Selatan (Richardo & Richie, 2019).

METHODS OF RESEARCH

The population in this research encompasses all cyber intelligence stakeholders responsible for cybersecurity in the cyber domain in Indonesia. The research sample constitutes a subset of this total population, selected to allow for generalizations about the entire population, thus requiring representation. The determination of the sample size and sampling technique is crucial in this regard.

For this research, the calculation of the sample size is based on a formula, assuming that the exact number of population members is unknown. The study spanned a six-month period and involved 136 respondents associated with cyber defense governance in Indonesia.

As outlined by Sugiyono, research variables are essentially aspects that the researcher chooses to study in order to gather information and draw conclusions. In the context of this research, the variables include: Legal measures (X_1); Capacity building (X_2); Strengthening cyber defense governance (Y).

Quantitative data, characterized by numerical values, can be derived from measurements (yielding continuous variables) or calculations (resulting in discrete variables. This research utilizes two types of data: secondary data and primary data, contingent on the survey method employed. Secondary data is pre-existing information obtained and processed by other entities, typically in the form of published materials. On the other hand, primary data is gathered and processed directly from the source by an individual or organization.

As per Sekaran & Bougie, primary data collection involves four techniques: interviews, observations, questionnaires or surveys, and experiments. In the case of this research, survey techniques are employed, wherein questionnaires are distributed both in person and non-personally (via online channels), and respondents are required to complete them

Building on the background and problem formulation outlined earlier, the hypotheses in this research represent tentative assertions about the uncertain or provisional relationships between variables that require empirical validation. In essence, these hypotheses serve as statement whose accuracy is yet to be established and necessitate substantiation through the research process.

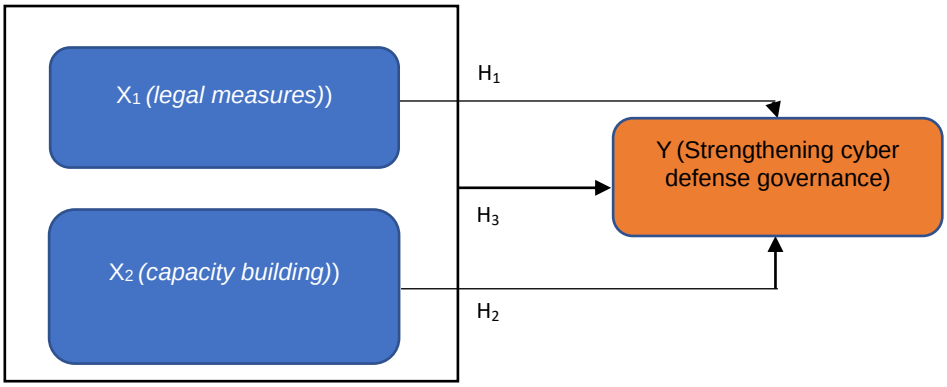

Figure 1 – Pattern of relationship between independent and dependent variables

Based on the problem formulation, theoretical studies, and previous research, the following research hypothesis was formulated:

- H1: There is an influence of legal certainty (legal measures) on strengthening cyber defense governance;
- H2: There is an influence of capacity building on strengthening cyber defense governance;
- H3: There is an influence of legal certainty (legal measures) and capacity building on strengthening cyber defense governance.

RESULTS AND DISCUSSION

A validity test is employed to assess the degree to which an instrument, serving as a measuring tool, accurately measures what it is intended to measure. In the context of a questionnaire, validity is achieved when the statements within the questionnaire effectively reveal the intended aspects being measured. In other words, a questionnaire is considered valid when its content aligns with and accurately reflects the constructs or variables it aims to assess. Validity testing is crucial to ensure that the questionnaire is a reliable and accurate tool for collecting meaningful data in the research context.

Table 1 – Validity test of legal measures (X1)

Statement	*Legal measures Factors* (X1)		
	rcount	rtable (N = 136)	information
X1.1	0,647	0,1672	Valid
X1.2	0,687	0,1672	Valid
X1.3	0,734	0,1672	Valid
X1.4	0,728	0,1672	Valid
X1.5	0,696	0,1672	Valid
X1.6	0,683	0,1672	Valid
X1.7	0,805	0,1672	Valid
X1.8	0,824	0,1672	Valid

It appears there may be a reference to a specific table that includes calculated correlation coefficients (r values) for each indicator item related to the legal certainty variable (X1). The statement suggests that, based on this table, all the indicator items within the legal certainty variable are considered valid. The reason cited is that the calculated r values for each indicator item exceed the critical r table value (0.1672) for the given sample size (N = 136).

In the context of validity testing, it's common to compare calculated correlation coefficients with critical values to determine whether the relationship between variables is statistically significant. If all calculated r values for the legal certainty variable surpass the critical threshold, it implies that the statements within this variable are deemed valid indicators according to the chosen criteria.

Table 2 – Validity test of capacity building (X2)

Statement	*Capacity building factors* (X2)		
	rcount	Rtable (N = 136)	information
X2.1	0,820	0,1672	Valid
X2.2	0,736	0,1672	Valid
X2.3	0,744	0,1672	Valid
X2.4	0,719	0,1672	Valid
X2.5	0,769	0,1672	Valid
X2.6	0,837	0,1672	Valid
X2.7	0,760	0,1672	Valid

It seems that there is a reference to a specific table containing calculated correlation coefficients (r values) for each indicator item related to the capacity building variable (X2). The conclusion drawn from this table is that all statements within the capacity building variable are considered valid. This determination is based on the observation that the calculated r values for all indicator items surpass the critical r table value (0.1672) for the given sample size (N = 136).

In the context of validity testing, surpassing the critical threshold for correlation coefficients suggests that the relationships between the items in the capacity building variable are statistically significant. This outcome supports the validity of the statements within this variable according to the chosen criteria.

Table 3 – Validity test of strengthening cyber defense governance (Y)

Statement	Strengthening cyber defense governance (Y)		
	rcount	Rtable (N = 136)	information
Y1	0,884	0,1672	Valid
Y2	0,854	0,1672	Valid
Y3	0,864	0,1672	Valid
Y4	0,844	0,1672	Valid
Y5	0,784	0,1672	Valid
Y6	0,787	0,1672	Valid
Y7	0,803	0,1672	Valid

The statement suggests that, based on a specific table, it can be concluded that all statements within the variable "Strengthening cyber defense governance" (Y) are valid. This conclusion is drawn because the calculated correlation coefficients (r values) for all indicator items in this variable exceed the critical r table value (0.1672) for the given sample size (N = 136).

In the context of validity testing, when the calculated r values for all indicator items surpass the critical threshold, it indicates that the relationships between the items in the variable are statistically significant. This outcome supports the validity of the statements within the "Strengthening cyber defense governance" variable, according to the chosen criteria.

The Reliability Test, often assessed using Cronbach's Alpha, is a statistical method employed to evaluate the consistency and reliability of a set of questionnaire items in measuring a specific variable. Cronbach's Alpha assesses the internal consistency of the items, indicating the degree to which they consistently measure the same underlying construct. A higher Cronbach's Alpha value suggests greater reliability among the items in capturing the intended variable, while a lower value may indicate less internal consistency. This test is crucial for ensuring that the measurement instrument reliably measures the construct of interest in a consistent manner.

Table 4 – Reliability Test of Legal measures (X1)

Reliability Statistics	
Cronbach's Alpha	N of Items
,871	8

The statement suggests that based on the values presented in Table 3.4, a reliability test was conducted for the legal certainty variable (X1) using Cronbach's Alpha. The calculated Cronbach's Alpha value is reported as 0.871, and it is compared to the critical value (r table) of 0.1672 for the given sample size (N = 136).

The conclusion drawn is that the Cronbach's Alpha value (0.871) is greater than the critical value (0.1672), indicating that the research instrument related to the legal certainty variable (X1) is considered reliable. In this context, reliability refers to the consistency and dependability of the instrument in measuring the legal certainty construct. A Cronbach's Alpha value above a certain threshold, in this case, 0.871, suggests a high level of internal consistency and reliability for the items within the legal certainty variable.

Table 5 – Reliability Test of Capacity building (X2)

Reliability Statistics	
Cronbach's Alpha	N of Items
,882	7

The statement indicates that a reliability test was conducted for the capacity building variable (X2) using Cronbach's Alpha, and the results are presented in a table. The calculated Cronbach's Alpha value is reported as 0.882, and it is compared to the critical value (r table) of 0.1672 for the given sample size (N = 136).

The conclusion drawn is that the Cronbach's Alpha value (0.882) is greater than the critical value (0.1672), implying that the research instrument related to the capacity building variable (X2) is considered reliable. In this context, reliability suggests that the items within the capacity building variable exhibit a high level of internal consistency and can be trusted to measure the intended construct consistently.

Table 6 – Reliability Test of strengthening cyber defense governance (Y)

Reliability Statistics	
Cronbach's Alpha	N of Items
,924	7

The statement indicates that a reliability test was conducted for the variable "Strengthening cyber defense governance" (Y) using Cronbach's Alpha, and the results are presented in a table. The calculated Cronbach's Alpha value is reported as 0.948, and it is compared to the critical value (r table) of 0.1672 for the given sample size (N = 136).

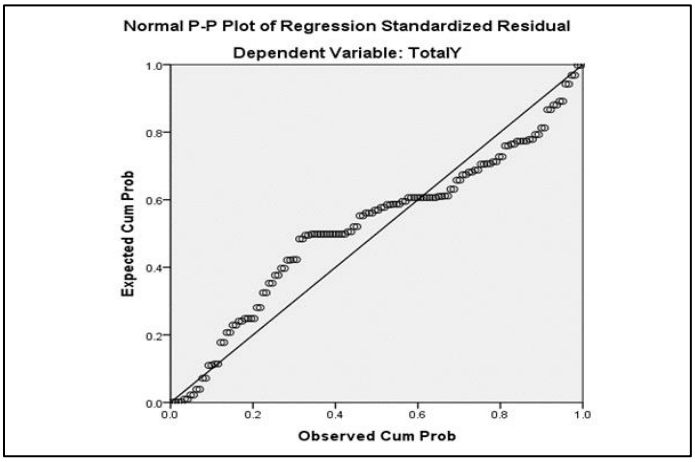

Figure 2 – Regression Plotting Graph of Dependent Variable: Y

The conclusion drawn is that the Cronbach's Alpha value (0.948) is significantly greater than the critical value (0.1672), suggesting that the research instrument related to the variable "Strengthening cyber defense governance" (Y) is considered highly reliable. This implies a high level of internal consistency among the items within the variable, indicating that the instrument can be trusted to measure the intended construct consistently.

It seems like there might be missing information regarding the results of the normality test. If you provide the specific results or statistics from the normality test, I can assist you in interpreting the findings and determining whether the data used in the regression model is normally distributed.

It appears that you haven't provided the specific results or statistics from the multicollinearity test. If you share the relevant information from the test, such as correlation coefficients or variance inflation factors (VIF), I can help you interpret the findings and assess whether there is a significant issue with multicollinearity among the independent variables in your regression model.

Table 7 – Multicollinearity Test

Coefficients[a]

Model		Collinearity Statistics	
		Tolerance	VIF
1	Total X1	.438	2.282
	Total X2	.438	2.282

a. Dependent Variable: Total Y

The information provided indicates that a multicollinearity test was conducted for the independent variables X1 and X2, and the results are presented in Table 4.14. According to the criteria specified, a Tolerance value greater than 0.1 and a VIF (Variance Inflation Factor) less than 10 are considered acceptable, suggesting no significant multicollinearity issues.

Specifically, the Tolerance value for the independent variables X1 and X2 is reported as 0.438, which is greater than the threshold of 0.1. Additionally, the VIF value is stated as 2.282, which is less than the threshold of 10. Based on these results, the conclusion is drawn that there is no intercorrelation between the independent variables X1 and X2. Therefore, the assumption of no symptoms of multicollinearity can be considered fulfilled, contributing to the validity of the regression model.

Table 8 – t Test Results Partial Test Results for Variables X1 and Y

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	7.348	1.612		4.558	.000
	Total X1	.298	.069	.347	4.321	.000
	Total X2	.450	.073	.496	6.182	.000

a. Dependent Variable: Total Y

Table 9 – t Test Results Partial Test Results for Variables X2 and Y

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	7.348	1.612		4.558	.000
	Total X1	.298	.069	.347	4.321	.000
	Total X2	.450	.073	.496	6.182	.000

a. Dependent Variable: Total Y.

Simultaneous Tests are carried out to see the influence between all independent variables and the dependent variable together.

It seems that you are describing the model test results, specifically focusing on the coefficient of determination (R^2), which is a measure of how well the independent variables

(X1 and X2) explain the variability in the dependent variable (Y). To provide a more detailed analysis or interpretation, I would need the specific values or statistics from the table of model test results. If you can provide the R^2 value and any other relevant information from the table, I can help you understand the extent to which the independent variables contribute to explaining the variation in the dependent variable.

Table 10 – Simultaneous Tests result

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1044.835	2	522.418	110.600	.000[b]
	Residual	628.223	133	4.723		
	Total	1673.059	135			

a. Dependent Variable: Total Y
b. Predictors: (Constant), TotalX2, Total X1.

Table 11 – The model test result

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.790[a]	.625	.619	2.17336

a. Predictors: (Constant), TotalX2, X1total
b. Dependent Variable: TotalY

The coefficient of determination (R^2) value of 0.619 suggests that approximately 61.9% of the variability in the dependent variable "Strengthening cyber defense governance" (Y) can be explained by the independent variables "Legal certainty factors" (X1) and "Capacity building factors" (X2). This indicates a relatively strong ability of the legal certainty and capacity building factors to influence and account for the observed changes in cyber defense governance.

In practical terms, a coefficient of determination close to 1 indicates a high degree of explanatory power, implying that a substantial portion of the variability in the dependent variable is captured by the independent variables. However, it's also worth noting that there may be other factors not included in the model that contribute to the remaining 38.1% of unexplained variability in "Strengthening cyber defense governance".

To carry out hypothesis testing H1, first calculate ttable as follows: ttable = t(α/2; n-k-1) = 1.65639. If the Sig value < 0.05 and tcount > ttable, then H0 is rejected and H1 is accepted. Obtained: 0.000 < 0.05 and 4.321 > 1.65639, then H0 is rejected and H1 is accepted. This means that there is an influence of legal certainty factors on strengthening cyber defense governance.

To carry out hypothesis testing H2, first calculate ttable as follows: ttable = t(α/2; n-k-1) = 1.65639. If the Sig value < 0.05 and tcount > ttable, then H0 is rejected and H2 is accepted. Obtained: 0.000 < 0.05 and 6.182 > 1.65639, then H0 is rejected and H2 is accepted. This means that there is an influence of capacity building factors on strengthening cyber defense governance.

To carry out hypothesis testing H3, first calculate ftable as follows: Ftable = F(k; n-k) = 3.06. If the Sig value < 0.05 and Fcount > Ftable, then H0 is rejected and H3 is accepted. Obtained: 0.000 < 0.05 and 110.600 > 3.06, then H0 is rejected and H3 is accepted. This means that there is a simultaneous influence of legal certainty factors and capacity building factors on strengthening cyber defense governance.

Table 12 – Multiple Linear Regression Test Results

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	7.348	1.612		4.558	.000
	strengthening cyber defense governance	.298	.069	.347	4.321	.000
		.450	.073	.496	6.182	.000

a. Dependent Variable: Strengthening cyber defense governance

Based on the table above, data analysis using SPSS 27 above, the results of the regression equation are obtained as follows:

$$Y = 7{,}348 + 0{,}298\ X1 + 0{,}450\ X2 + e$$

The provided analysis of the multiple linear regression equation offers several conclusions regarding the relationships between the independent variables (Legal certainty Factors and Capacity Building factors) and the dependent variable (Strengthening cyber defense governance).

Here are the summarized conclusions:

- Constant Value (Intercept): The constant value is 7.348, indicating that if there is no change in the variables Legal certainty Factors and Capacity Building factors (assuming X1 and X2 values are both 0), then the predicted value for Strengthening cyber defense governance is 7.348 units;
- Regression Coefficient for Legal Certainty Factors (X1): The regression coefficient for Legal certainty Factors (X1) is 0.298. This means that if the Legal certainty Factors variable increases by 1%, assuming Capacity Building factors (X2) and the constant (a) are both 0, then strengthening cyber defense governance is predicted to increase by 0.298 units. The positive coefficient suggests that an improvement in legal certainty Factors contributes positively to strengthening cyber defense governance;
- Regression Coefficient for Capacity Building Factors (X2): The regression coefficient for Capacity Building factors (X2) is 0.450. This indicates that if the Capacity Building factors variable increases by 1%, assuming Legal certainty Factors (X1) and the constant (a) are both 0, then strengthening cyber defense governance is predicted to increase by 0.450 units. Similar to legal certainty Factors, a positive coefficient implies that an enhancement in capacity building Factors contributes positively to strengthening cyber defense governance;
- Overall Contribution: The analysis suggests that both Legal certainty Factors and Capacity Building factors implemented positively contribute to strengthening cyber defense governance. This finding challenges assumptions that question the effectiveness of these factors in enhancing cyber defense governance. The conclusion emphasizes the importance of considering legal certainty and capacity building factors in the planning stage to achieve the desired outcomes in strengthening cyber defense governance in Indonesia.

CONCLUSION

Indeed, based on the comprehensive explanation starting from the background, problem formulation, and quantitative data analysis, the following conclusions can be drawn:

- Influence of Legal Certainty Factors: There is a discernible influence between legal certainty factors and the strengthening of cyber defense governance in Indonesia. This is supported by the quantitative analysis, indicating a statistically significant relationship between legal certainty factors and the dependent variable;
- Influence of Capacity Building Factors: There is also a noteworthy influence between capacity building factors and the strengthening of cyber defense governance in Indonesia. The quantitative analysis substantiates this conclusion by demonstrating a statistically significant association between capacity building factors and the dependent variable;
- Positive Contribution of Implemented Factors: The multiple linear regression equation analysis reinforces the idea that the implemented legal certainty factors and capacity building factors positively contribute to the strengthening of cyber defense governance in Indonesia. This implies that improvements or enhancements in these factors can positively impact the effectiveness of cyber defense measures in the country.

In summary, the study suggests that addressing legal certainty factors and enhancing capacity building factors can play a vital role in bolstering cyber defense governance in Indonesia, highlighting the significance of these factors in the overall cybersecurity framework.

ACKNOWLEDGEMENTS

This research is supported by the University of Brawijaya, Malang. The authors also express many thanks to the respondents who have provided information regarding strategies and the influence of strengthening cyber defense governance in Indonesia.

REFERENCES

1. Andress, J., & Winterfeld, S. (2014). Cyber Warfare: Techniques, Tactics and Tools for Security Practicioners. Waltham: Esevier.
2. Brantly, A. (2013). Defining the role of intelligence in cyber: A hybrid push and pull. Understanding the Intelligence Cycle, pp. 76 - 98. Oxon: Routledge.
3. Caplan, N. (2013). Cyber War: the Challenge to National Security. Global Security Studies, 4 (1), 93 -115.
4. David, & R., F. (2011). Strategic Management: Concepts and Cases. New Jersey: Prentice Hall.
5. Garrick, J., & Ghan, A. L. (2004). University-industry partnerships: implication for industrial training, opportunities for new knowledge. Journal of European Industrial Training, 28 (2-4), 329-338.
6. Marsetio. (2016). Diplomasi Siber Dalam Mendukung Poros Siber Dunia.
7. Richardo, & Richie, M. (2019). Kepentingan Kebijakan Politik Luar Negeri Freedom Of Navigation Amerika Serikat Terhadap Sengketa di Laut China Selatan. JOM Fisip Universitas Riau, Vol. 6 Edisi II.
8. Roell, Peter, Lurtz, Feldt, & Thiele, R. D. (2013). Cyber Security: Perspective for A Comprehensive Approach. ISPSW Strategies Series: Focus on Defense and International Security., No. 222 Apr 2013.
9. Sani, C. L. (2013). Data Collection Technique a Guide for Researchers in HUmanities and Education. International Research Journal of Computer Science and Information Systems, pp. 40-42.
10. Sundarakani, B., Sikdar, A., & Balasubramanian, S. (2014). System Dynamics-based Modelling and Analysis of Greening the Construction Industry Supply Chain. International Journal of Logistics Systems and Management, 18(4), pp. 517-537.
11. Tan, W., & Subramaniam. (2005). Egovernment: Implementation Policies and Best Practices from Singapore. Electronic Government Strategies and Implementation, hh. 305-324.
12. Uthoff, C. (20115). Strategic Cyber Intelligence: An examination of Practices across Industry, Government, and Military. Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice. Hampshire: Palgrave Macmi.
13. Zhao, J., J., & Zhao, S. Y. (2010). “Opportunities and Threats: A Security Assessment of State EGovernment Websites”. Government Information Quarterly, vol. 27(1), hh. 49-56.
14. Zheng. (2015). From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond. China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, pp. 123 - 128.